Laboratory for Information and Decision Systems
Department of Electrical Engineering and Computer Science
Massachusetts Institute of Technology
Cambridge, Massachusetts 02139

STATUS REPORT NUMBER TWO, ON THE DEVELOPMENT OF A METHODOLOGY FOR THE DETECTION OF SYSTEM FAILURES AND FOR THE DESIGN OF FAULT-TOLERANT CONTROL SYSTEMS

ONR CONTRACT NO. N00014-77-C-0224

Report LIDS-SR-873
November 1, 1977 through November 30, 1978

To: Dr. Stuart Brodsky, Code 432
Office of Naval Research
Room 607
800 North Quincy Boulevard
Arlington, Virginia

December 27, 1978

SUMMARY

A brief description of the research carried out by faculty, staff, and students of the M.I.T. Laboratory for Information and Decision Systems under ONR Contract N00014-77-C-0224 is described. The period covered in this status report is from November 1, 1977 through November 30, 1978.

The scope of this contract is the development of an overall failure detection system design methodology and the study of closed-loop adaptive control system design techniques that are fault-tolerant. In the following sections we overview the research that has been performed in these areas during the indicated time period. We have also included a list of the papers that have been and are being written as a result of research performed under this contract.

I. Analysis of the Multiple Model Adaptive Control (MMAC) Algorithm

One of the primary motivations for research in the area of failure detection is for the design of high-performance, very reliable feedback control systems. In such a closed-loop system the failure detection system affects overall behavior by switching on and off different feedback loops. For example, if a failure is detected in a particular sensor or actuator, the appropriate back-up might be activated or the feedback compensator might be reconfigured to get by without this instrument. It is also possible to perform this "switching" probabilistically. In such a system we discount the worth of a particular instrument as the probability that it has failed increases. Such feedback systems have the potential for improving system performance, but the presence of switches can lead to stability problems.

As reported in [4], the MMAC algorithm has exhibited instabilities in applications and in some initial work performed under this contract in the preceding year. During this past year we have expanded our analysis and have developed a number of insights into the performance of closed-loop MMAC systems and have devised analytical tools which should be of value in studying a variety of types of feedback systems with switches. This work is presented in detail in [1,3]. In the following development, we will sketch the main ideas.

Recall the basic MMAC formulation. We will write the equations in both continuous - and discrete-time. The open loop system is assumed to be linear

$$\dot{x}(t) = Ax(t) + Bu(t) + w(t) \tag{1}$$

$$y(t) = Cx(t) + v(t) \tag{2}$$

or

$$x(k+1) = Ax(k) + Bu(k) + w(k) \tag{3}$$

$$y(k) = Cx(k) + v(k) \tag{4}$$

where $x \in R^n$, $u \in R^m$, $y \in R^p$, and w and v are independent white noise processes, with

$$E[w(t)w'(\tau)] = Q\delta(t-\tau), \quad E[v(t)v'(\tau)] = R\delta(t-\tau) \tag{5}$$

$$E[w(k)w'(j)] = Q\delta_{kj}, \quad E[v(k)v'(j)] = R\delta_{kj} \tag{6}$$

While the open-loop system is assumed to be linear, it is not assumed to be known. Instead, a set of possible models are postulated

$$\dot{x}_i(t) = A_i x_i(t) + B_i u(t) + w_i(t) \tag{7}$$

$$y(t) = C_i x_i(t) + v_i(t) \tag{8}$$

$$w_i \sim Q_i, \quad v_i \sim R_i \tag{9}$$

$$x_i(k+1) = A_i x_i(k) + B_i u(k) + w_i(k) \tag{10}$$

$$y(k) = C_i x_i(k) + v_i(k) \tag{11}$$

$$w_i \sim Q_i, \quad v_i \sim R_i \tag{12}$$

i=1,...,N.

If one designs Kalman filters for each of these models, one can use the filter residuals (innovations processes) to compute the conditional

probability $p_i(t)$ or $p_i(k)$ for the validity of the ith model given all of the data up to time t or k, and assuming that one of the n models is correct. If we use steady-state Kalman filters, we obtain

$$\hat{x}_i(k+1) = A_i\hat{x}_i(k) + B_iu(k) + H_ir_i(k+1) \tag{13}$$

$$r_i(k+1) = y(k+1) - C_i[A_i\hat{x}_i(k) + B_iu(k)] \tag{14}$$

where H_i is the Kalman gain for the ith model

$$H_i = \sum_i C_i' R_i^{-1} \tag{15}$$

and $\sum_i$ is the solution to the Riccati equation

$$\sum_i = [C_i' R_i^{-1} C_i + (A_i \sum_i A_i' + Q_i)^{-1}]^{-1} \tag{16}$$

Assuming that the actual system matches the ith model, then $r_i(k)$ is a zero mean, white process with covariance

$$\theta_i = C_i \sum_i C_i' + R_i \tag{17}$$

and the probabilities are obtained from the recursive equation

$$p_i(k+1) = \frac{p_i(k)f_i[r_i(k+1)]}{\sum_{j=1}^{N} p_j(k)f_j[r_j(k+1)]} \tag{18}$$

where $f_i(\cdot)$ is the probability density function for r_i assuming that the ith model is correct:

$$f_i(r) = \left(\sqrt{(2\pi)^m \det(\theta_i)}\right)^{-1} \exp- \left\{\frac{1}{2}\ r'\theta_i^{-1}r\right\} \tag{19}$$

In continuous-time, the equations become

$$\dot{\hat{x}}_i(t) + A_i\hat{x}_i(t) + B_iu_i(t) + H_ir_i(t) \tag{20}$$

$$r_i(t) = y(t) - C_i\hat{x}_i(t) \tag{21}$$

and, if the model is correct, r_i is zero-mean, white noise with strength R_i. The probabilities are then obtained from

$$\dot{P}_i(t) = p_i(t)\left[\left(\sum_{j=1}^{N} p_j(t)r_j(t)\right) - r_i(t)\right] R_i^{-1}\left(\sum_{j=i}^{N} p_j(t)r_j(t)\right) \tag{22}$$

Suppose we now assume that with each model we have associated a feedback control law

$$u_i(t) = G_i\hat{x}_i(t) \tag{23}$$

or

$$u_i(k) = G_i\hat{x}_i(k) \tag{24}$$

Then, the MMAC algorithm specifies that the actual control be a probabilistically weighted sum of these

$$u_i(t) = \sum_{i=1}^{N} p_i(t)G_i\hat{x}_i(t) \tag{25}$$

$$u_i(k) = \sum_{i=1}^{N} p_i(k)G_i\hat{x}_i(k) \tag{26}$$

In most of the research reported in [1,3] attention is focussed upon a special case. This special case was chosen because it captures most of the essential features of the MMAC algorithm without adding unnecessary complexity. In this special case, N=2, $B=B_1=B_2 = C=C_1=C_2 = I$, $R_1=R_2=R$, $Q_1=Q_2=Q$. Thus, the only differences between the true system and the models are in the matrices A, A_1, A_2. Since in this case we have $p_2(t) = 1-p_1(t)$, we can rewrite the overall closed-loop system in a particularly useful form. Define

$$w(k) = \begin{bmatrix} x(k) \\ r_1(k) \\ r_2(k) \end{bmatrix} \tag{27}$$

Then

$$w(k+1) = \tilde{A}(p_1(k))w(k) \tag{28}$$

$$p_1(k+1) = \frac{p_1(k)f_1[r_1(k+1)]}{p_1(k)f_1[r_1(k+1)]+[1-p_1(k)]f_2[r_2(k+1)]} \tag{29}$$

where

$$\tilde{A}(p_1) = \left[\begin{array}{c|c|c} A-p_1G_1 - (1-p_1)G_2 & p_1G_1(I-H_1) & (1-p_1)G_2(I-H_2) \\ \hline A-A_1 & A_1(I-H_1) & 0 \\ \hline A-A_2 & 0 & A_2(I-H_2) \end{array}\right] \tag{30}$$

and in continuous time

$$\dot{w}(t) = \tilde{A}(p_1(t))w(t)$$

$$\dot{p}_1(t) = p_1(t)[1-p_1(t)][r_2(t)-r_1(t)]R^{-1}[p_1(t)r_1(t)+(1-p_1(t))r_2(t)] \quad (31)$$

where

$$\tilde{A}(p_1) = \left[\begin{array}{c|c|c} A-p_1G_1-(1-p_1)G_2 & p_1G_1 & (1-p_1)G_2 \\ A-A_1 & A_1-H_1 & 0 \\ A-A_2 & 0 & A_2-H_2 \end{array}\right] \quad (32)$$

Several comments are in order

(1) The system is decidedly nonlinear, but the "state" equation for w can be thought of as a linear system <u>modulated</u> by the value of p_1. Clearly the stability properties of $\tilde{A}(p_1)$ for fixed values of p_1 are of importance in the stability analysis of the overall system.

(2) The probability equations are such that if p_i ever is zero, it is zero from then on. This can be a problem in digital implementation. Thus, limits are placed on the probability

$$P_{LIM} \leq p_1(t) \leq 1 - P_{LIM} \quad (33)$$

We have used a value of $P_{LIM} = 10^{-50}$ in our simulations.

For most of the work reported in [1,3], this special model was specialized a bit further to obtain a form that both is amenable to analysis and that exhibits the several modes of behavior that are

characteristic of MMAC systems. This form is characterized by

$$A = \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}, \quad A_1 = \begin{bmatrix} a & 0 \\ 0 & \hat{a} \end{bmatrix}, \quad A_2 = \begin{bmatrix} \hat{a} & 0 \\ 0 & a \end{bmatrix} \tag{34}$$

The filter and control gains are also diagonal, by symmetry

$$H_1 = \begin{bmatrix} h & 0 \\ 0 & \hat{h} \end{bmatrix}, \quad H_2 = \begin{bmatrix} \hat{h} & 0 \\ 0 & h \end{bmatrix} \tag{35}$$

$$G_1 = \begin{bmatrix} g & 0 \\ 0 & \hat{g} \end{bmatrix}, \quad G_2 = \begin{bmatrix} \hat{g} & 0 \\ 0 & g \end{bmatrix} \tag{36}$$

Various modes of behavior are possible for this system. In the following pages we have included some plots for each of these from [1]. Each set of plots consists of three graphs. The first is of the probability $p_1(t)$, the second of $x_1(t)$ and $x_2(t)$, and the third of the quantity $\ell n[x_1(t)x_2(t)]$. We will comment on the significance of this quantity in a moment

Exponential Mode

The first set of figures (Figures 3.1a,b,c, from [1]) correspond to an example in which $\tilde{A}(p_1)$ is stable for all values of p_1. This is a rather strong condition, as it requires that each controller (for model 1 and for model 2) must stabilize the overall system by itself.

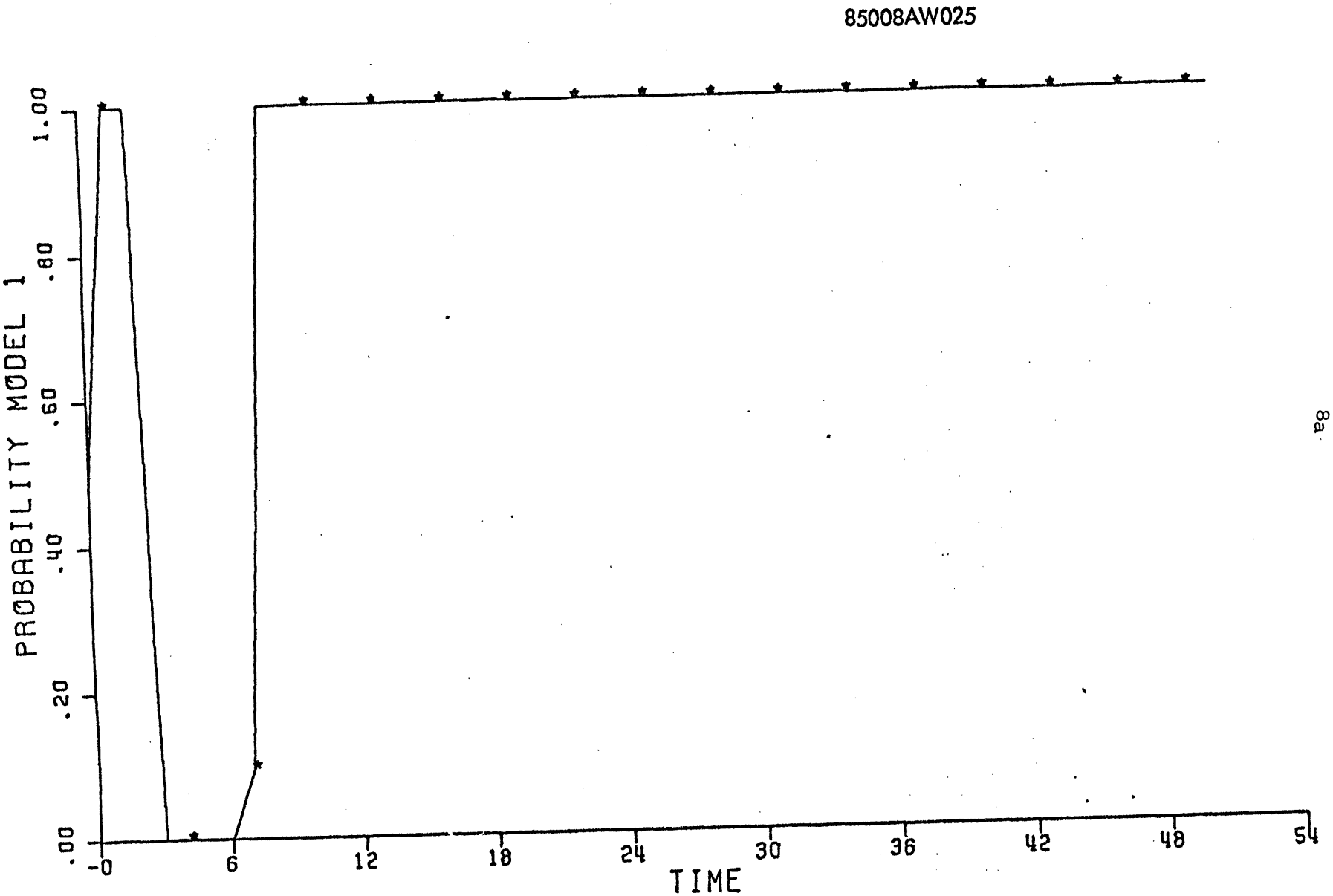


Fig. 3.1 Universally Stable Simulation
(Case 3)

a) Probability of Model 1

a) Probability of Model 1

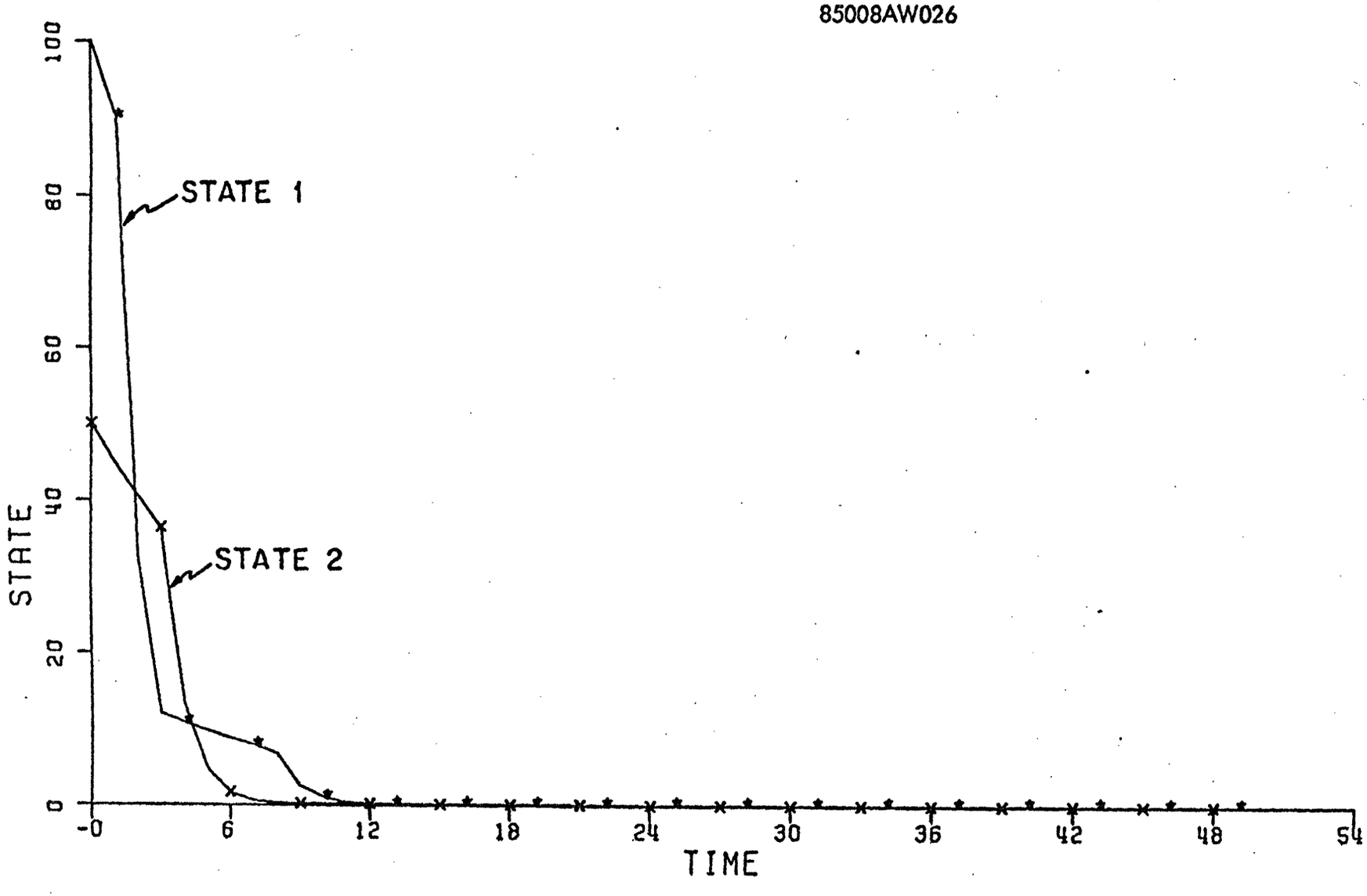


Fig. 3.1 Universally Stable Simulation
(Case 3)

b) True States

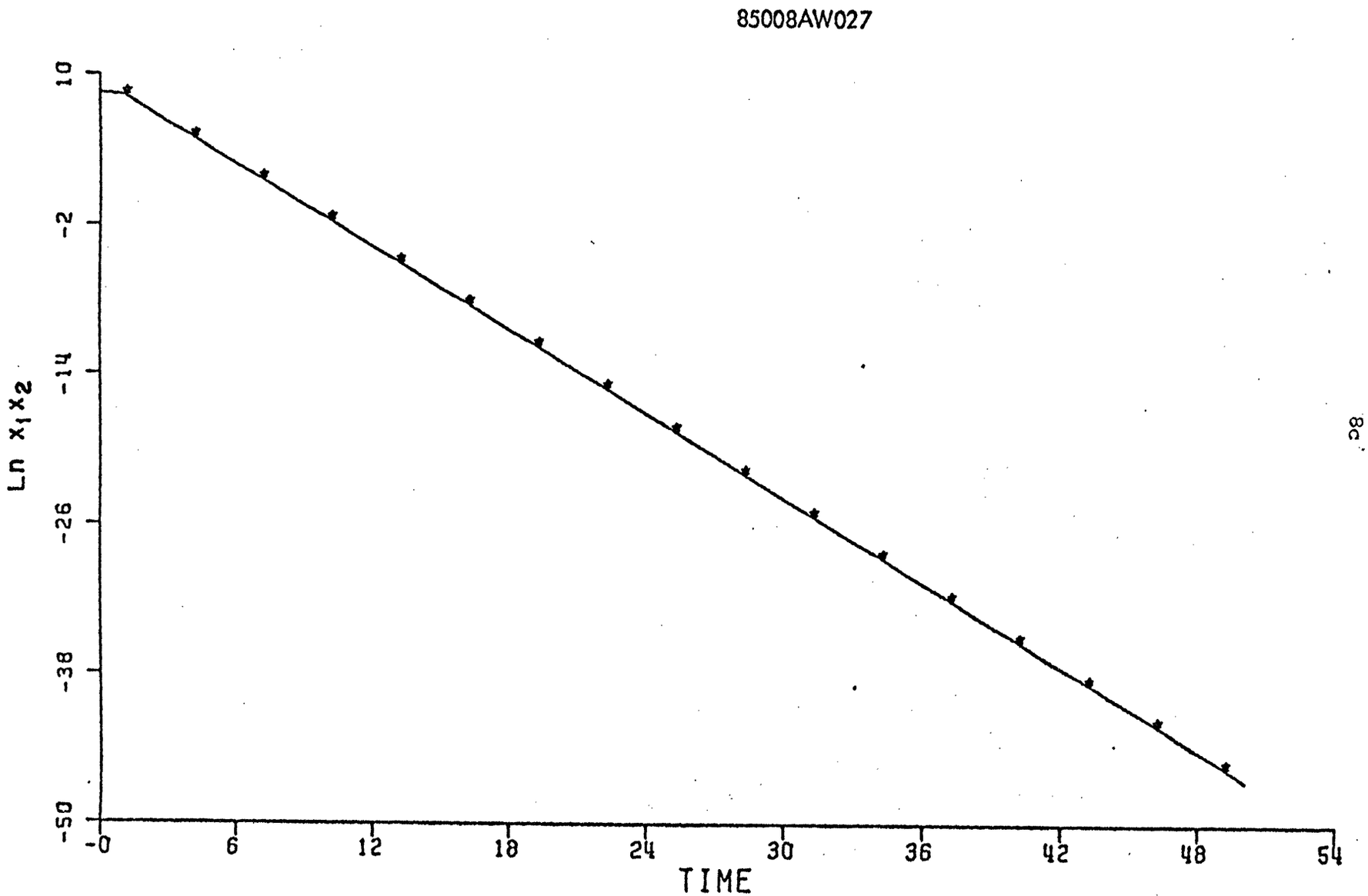


Fig. 3.1 Universally Stable Simulation
(Case 3)

c) Ln $x_1 x_2$

In this case, both x_1 and x_2 decay exponentially [1]. As illustrated in Figure 3.1a, the probability p_1 oscillator rather drastically. This is characteristic of the MMAC design. In this case, since the system is stable for all values of p_1, the probability eventually settles out at some value. Since when w is small, there is no information from which one can determine the validity of either model, the final value of p_1 cannot be determined -- it depends on the initial condition. This can also be seen from the neutral stability of the p_1 equation about the equilibrium point w=0, p_1=1/2 -- to first order there is no tendency for p_1 to return to 1/2 if it is perturbed [1]. This can also be seen from the probability equations (29), (31), in which we see that changes in p_1 depend upon $||r_i||^2$, which is zero to first order. This also illustrates one of the important stability problems with MMAC: since changes in x, r_1, r_2 depend upon $||r_i||$ and changes in p depend upon $||r_i||^2$, for small initial conditions, changes in p will lag changes in w, but if $||w||$ increases, p will change much faster than w. This leads to the switch-like behavior of the probability as seen in Figure 3.1a. This behavior can also be analyzed by rewriting the probability equation in the discrete-time case [1]:

$$p_1(k) = \frac{p_1(0)\tilde{\beta}\, e^{-1/2\alpha(k)}}{p_1(0)\tilde{\beta}\, e^{-1/2\alpha(k)} + (1-p_1(0))} \qquad (37)$$

where

$$\tilde{\beta} = \left(\frac{\det[\theta_2]}{\det[\theta_1]} \right)^{1/2} \tag{38}$$

and $\alpha(k)$ is the log-likehood ratio

$$\alpha(k) = \sum_{i=1}^{k} \left[r_1'(k) \theta_1^{-1} r_1(k) - r_2'(k) \theta_2^{-1} r_2(k) \right] \tag{39}$$

Figure 4.1a from [1] is a plot of $p_1(k)$ versus $\alpha(k)$ for a few values of $p(o)$ and $\tilde{\beta}=1$. From this, if we define α_s to be the value of $\alpha(\cdot)$ for which $P(\cdot)=1/2$

$$\alpha_s = -2 \ \ell n \left[\frac{1-P_o}{P_o \tilde{\beta}} \right] \tag{40}$$

we see that (37) behaves almost like a switch

$$\begin{aligned} \alpha(\cdot) > \alpha_s \quad &\Rightarrow p_1(\cdot) = 0 \\ \alpha(\cdot) < \alpha_s \quad &\Rightarrow p_1(\cdot) = 1 \end{aligned} \tag{41}$$

Oscillatory Response

The switch - type behavior of the probabilities leads to some of the most unusual characteristics of the MMAC responses. A great deal of analysis for this type of response is contained in [1]. Suppose that $\tilde{A}(p_1)$ is unstable for all values of p_1. Even with this, it is possible

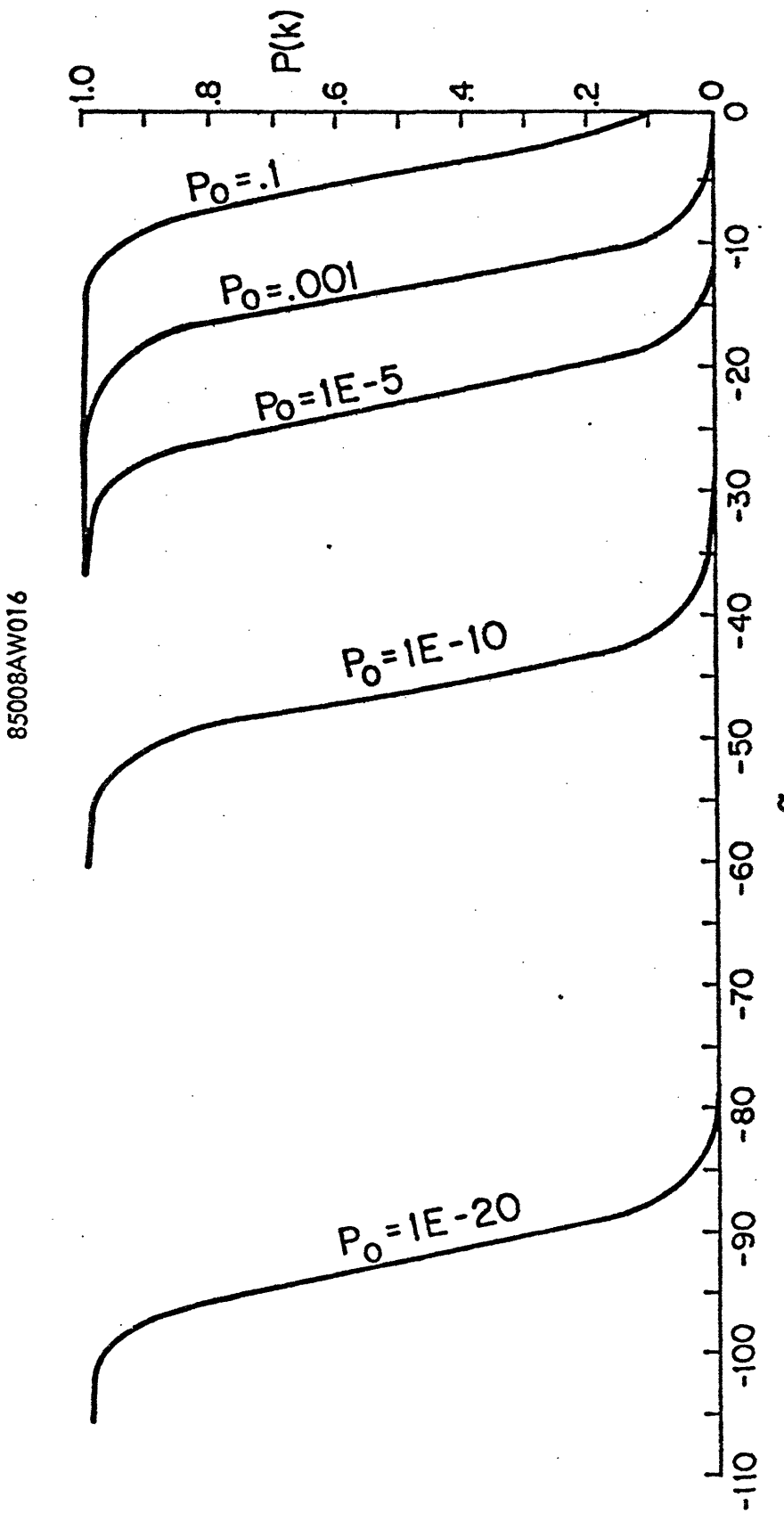


Fig. 4.1 Plot of P(•) versus α(°)

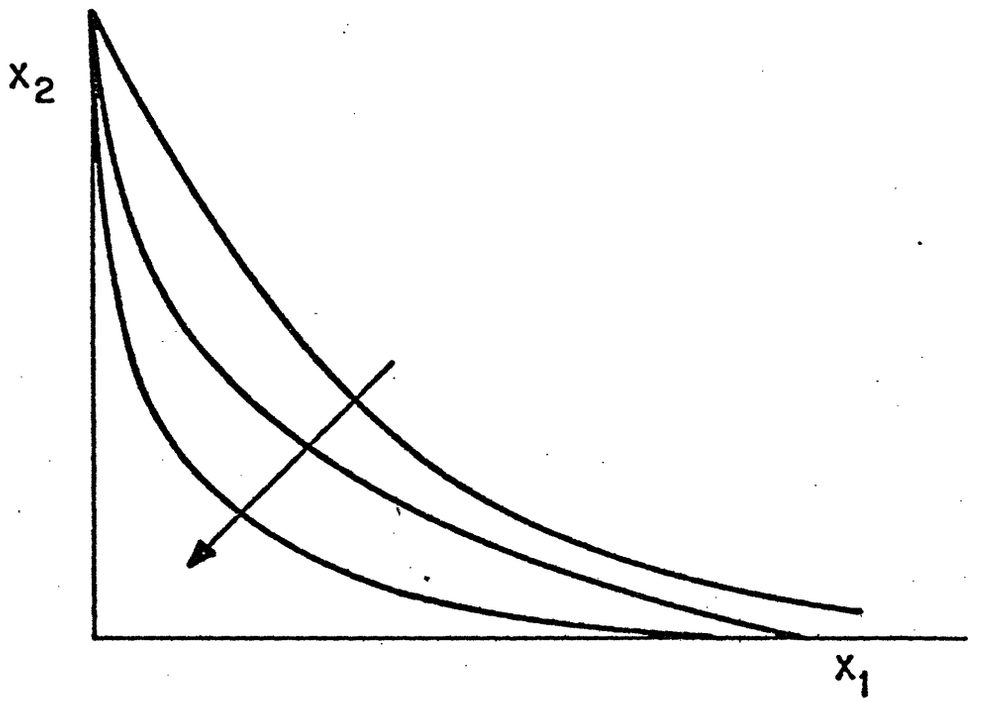
a) Various Values of P_0

to have an overall response that is stable. For our example, this is particularly simple to see. The controller for model 1 knows the dynamics of the first component of x perfectly and can thus stabilize its response, and the model 2 controller can do the same for x_2. Thus, one can imagine a stable overall response in which p_1 switches between 0 (actually P_{LIM}) and 1 ($1-P_{LIM}$), alternately stabilizing each state.

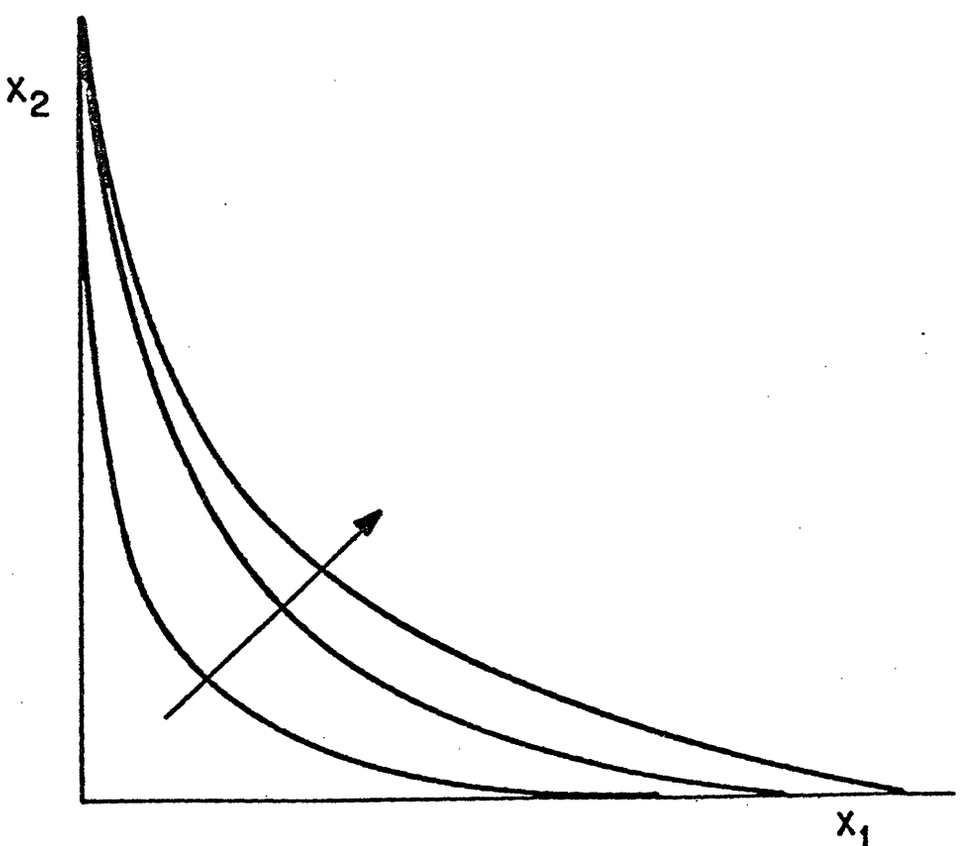
When the probabilities do oscillate, the overall response can be either stable, neutrally stable, or unstable. As discussed in [1], the factor that determines the overall behavior is the notion of hyperbolic stability. As mentioned above; MMAC alternately controls each of the two modes of the system (depending upon the value of p_1). Thus at any time one of the two states x_1 and x_2 is decaying exponentially, while the other is exponentially diverging. Thus the product of the two states is of the form

$$x_1 x_2 \sim e^{bt} \tag{42}$$

where $b>0$ occurs if states diverge faster when uncontrolled than they decay when controlled, while the reverse is true if $b<0$. Also, in this case we can think of the state as evolving along a family of hyperbolas, $x_1 x_2$=constant (see Figure 3.5). If $b<0$, we obtain the "hyperbolically stable" case, while if $b>0$, we have hyperbolic instability. In Figures 3.2, 3.3, 3.4 we have illustrated stable ($b<0$), neutrally stable ($b=0$), and unstable ($b>0$) cases. Note that although the separate trajectories for x_1 and x_2 are rather irregular, the product $x_1 x_2$ does behave



(a) Stable



(b) Unstable

Fig. 3.5 Phase-Plane Plot

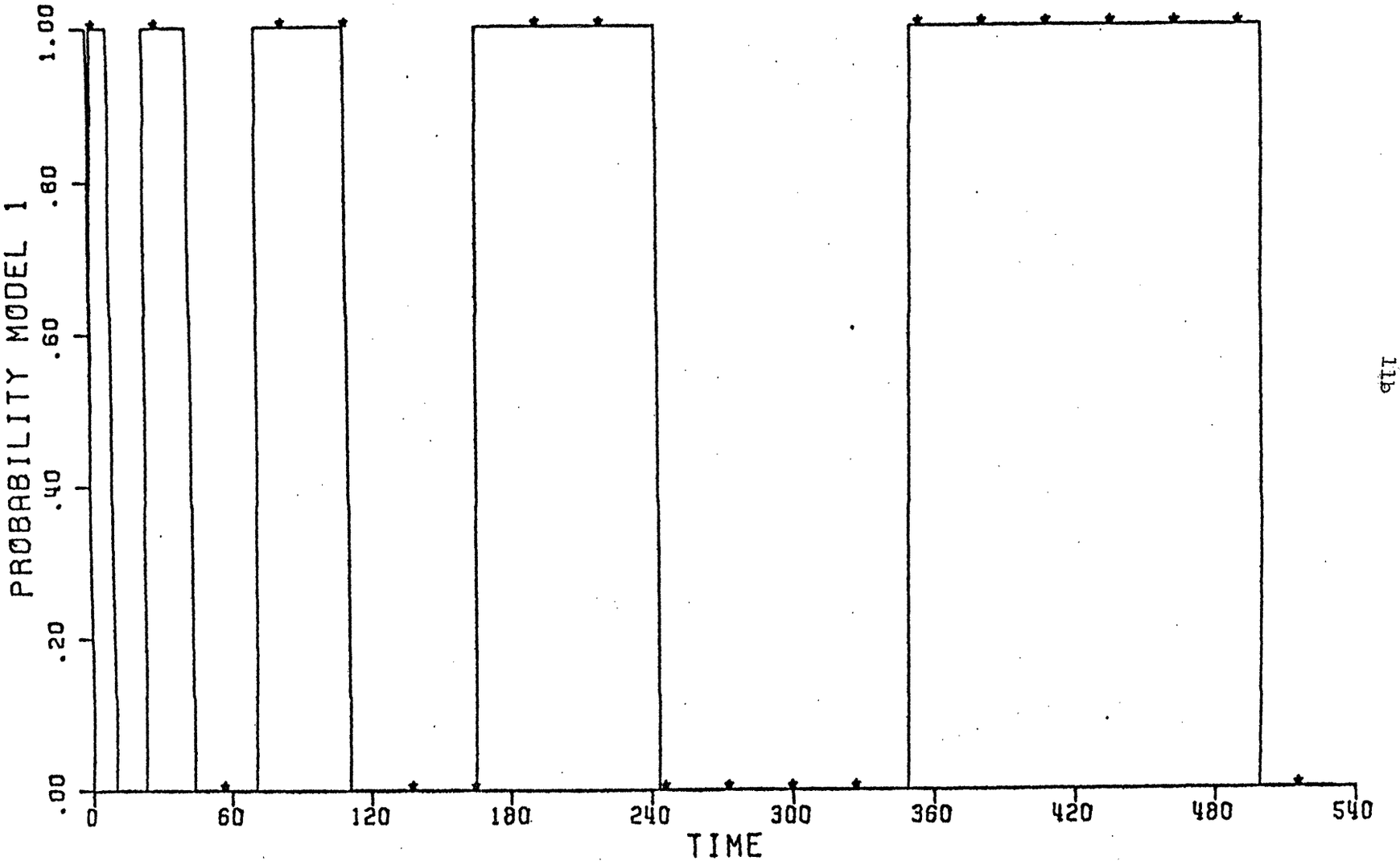


Fig. 3.2 Stable Oscillation
(Case 1a)

a) Probability of Model 1

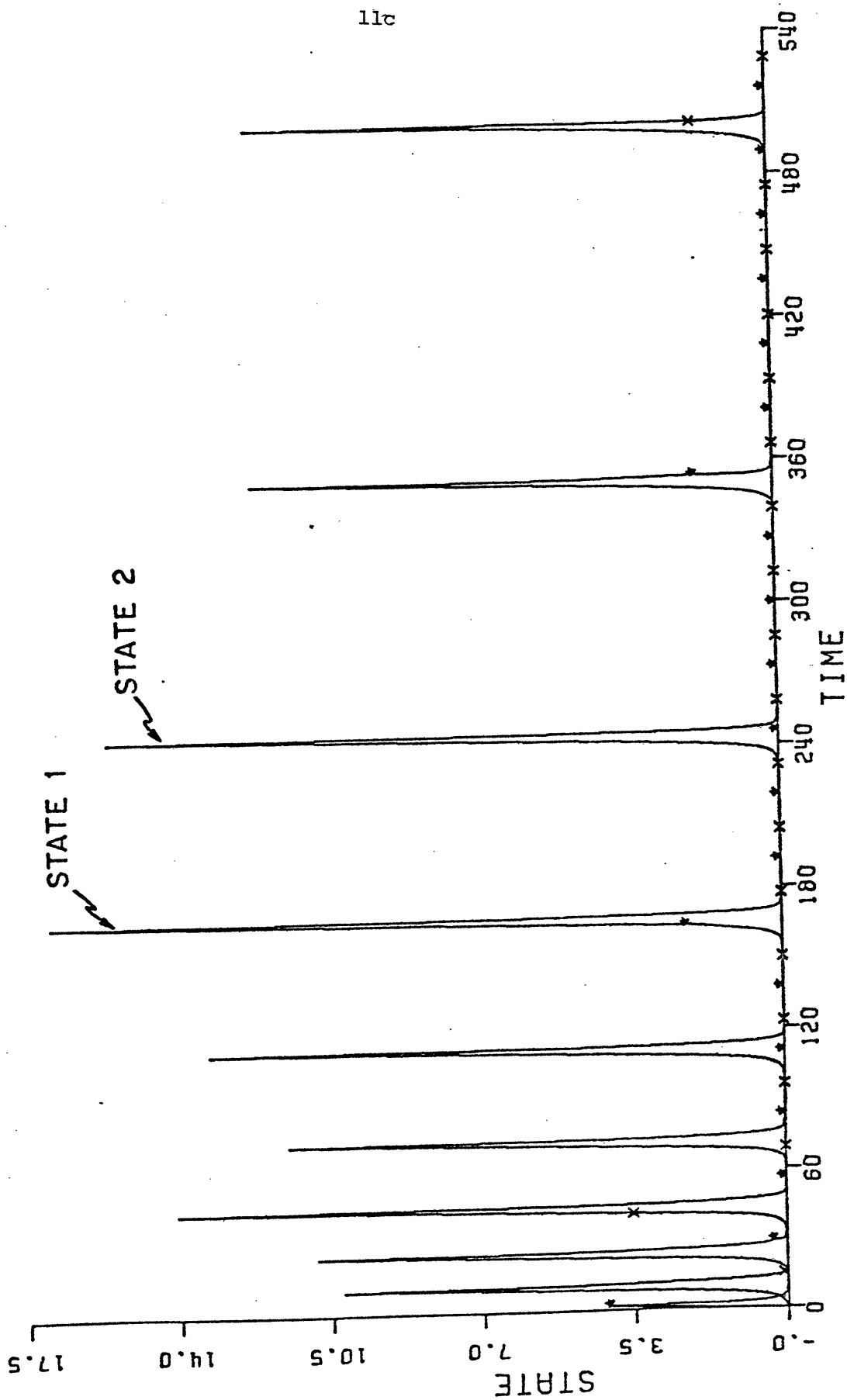


Fig. 3.2 Stable Oscillation
(Case 1a)

b) True States

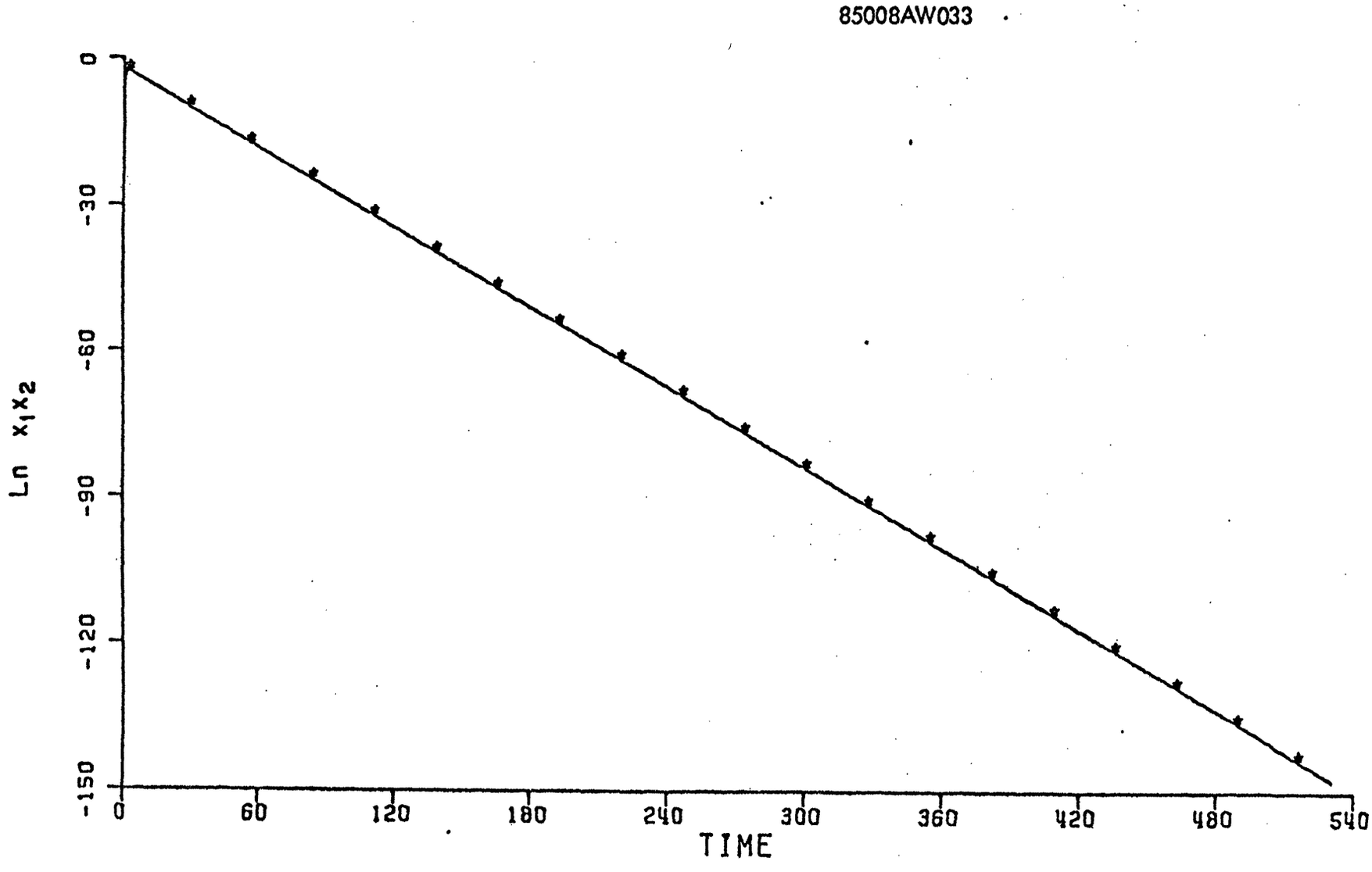
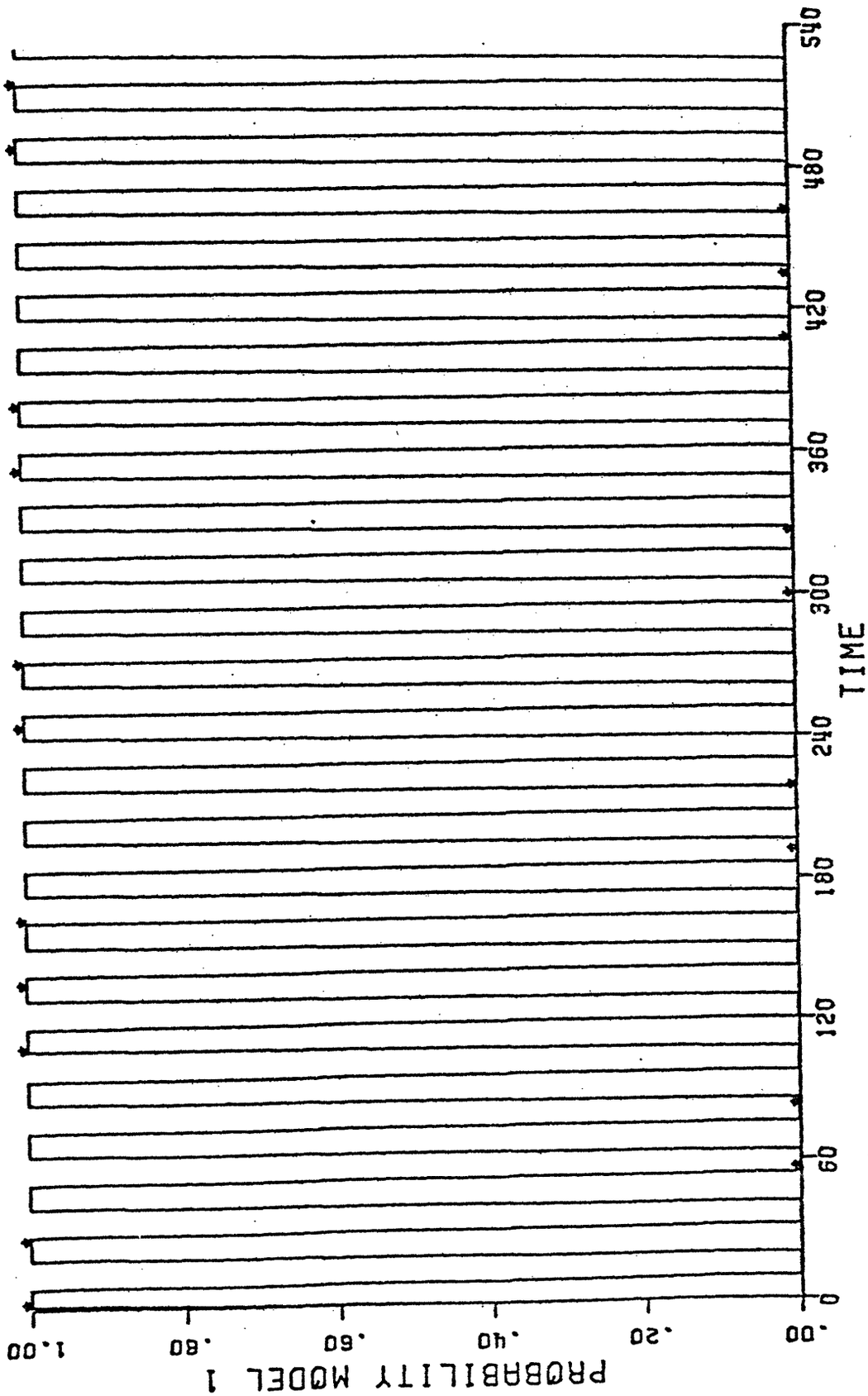


Fig. 3.2 Stable Oscillation
(Case 1a)

c) Ln x_1x_2



85008AW034

Fig. 3.3 Neutrally Stable Oscillation
(Case 1b)

a) Probability of Model 1

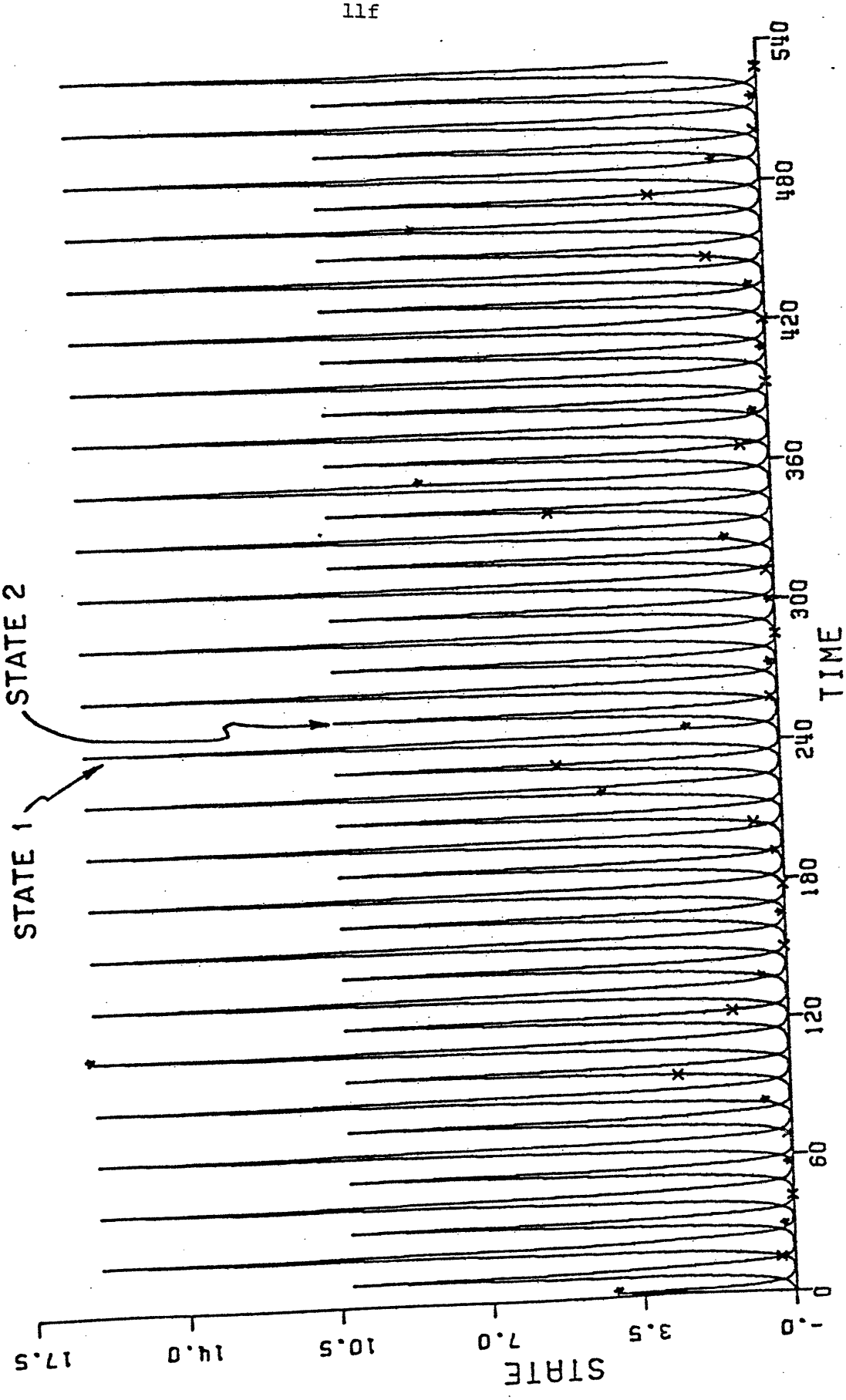


Fig. 3.3 Neutrally Stable Oscillation
(Case 1b)

b) True States

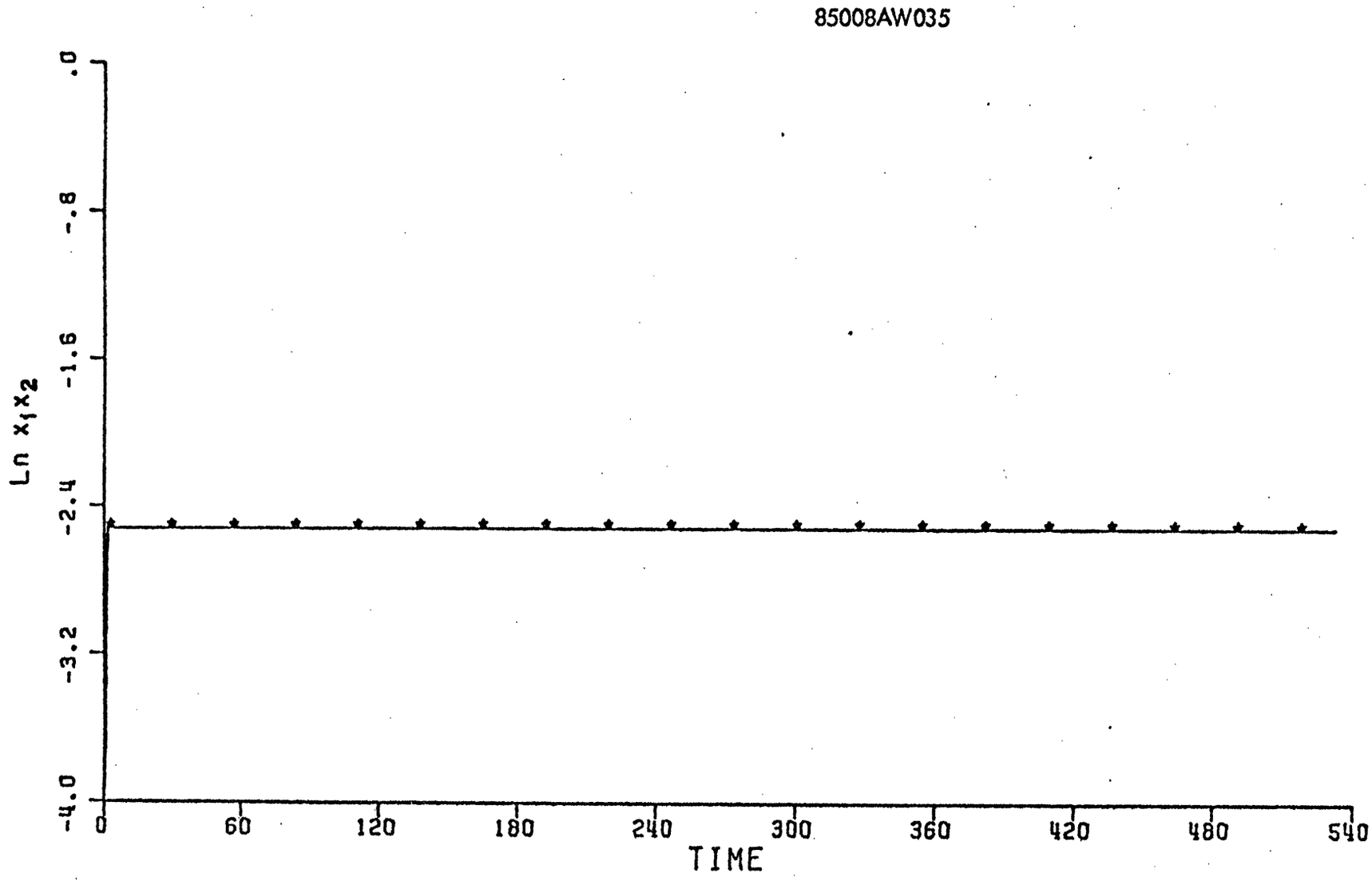


Fig. 3.3 Neutrally Stable Oscillation
(Case 1b)

c) Ln x_1x_2

85008AW036

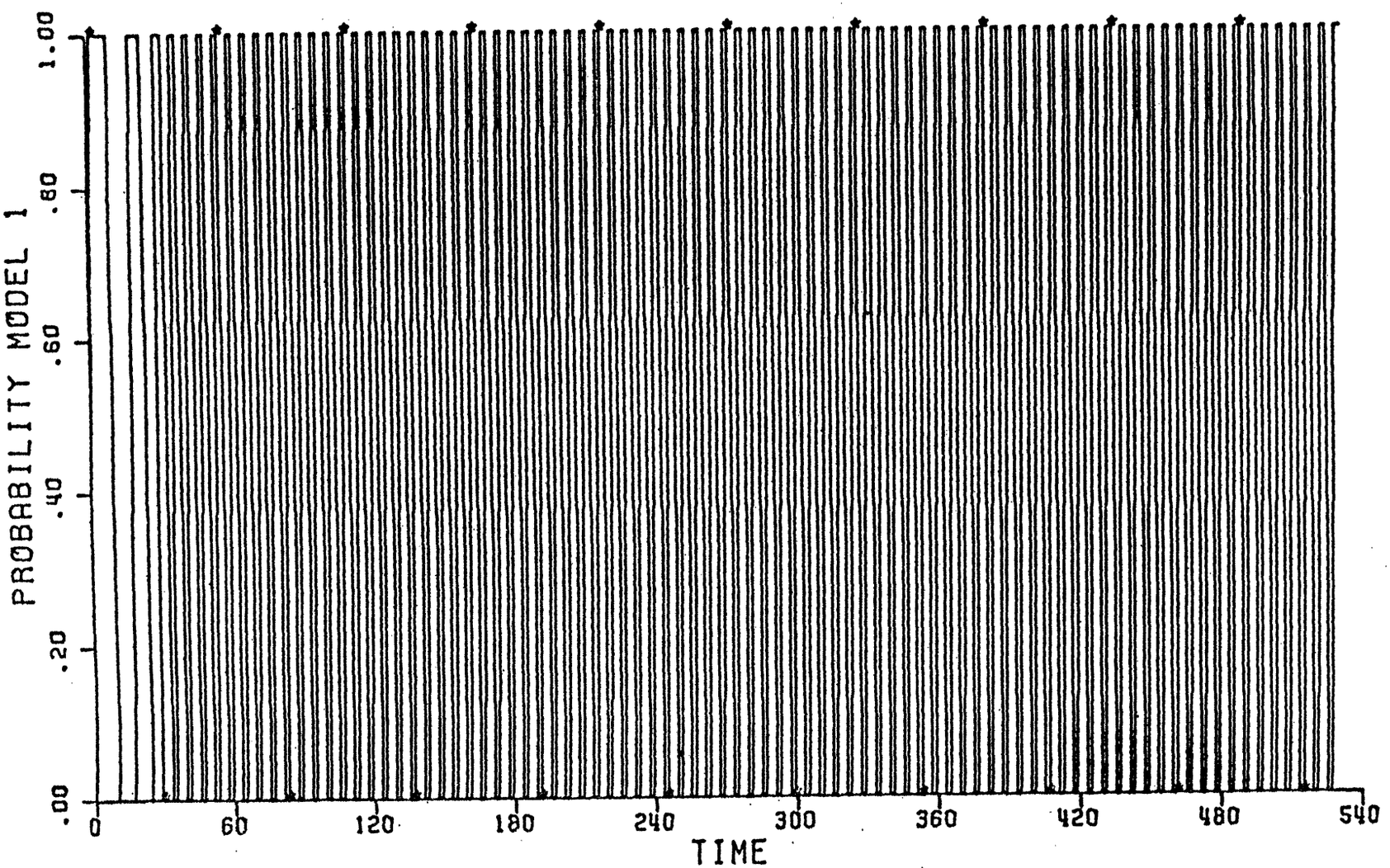


Fig. 3.4 Unstable Oscillation
(Case 1c)

a) Probability of Model 1

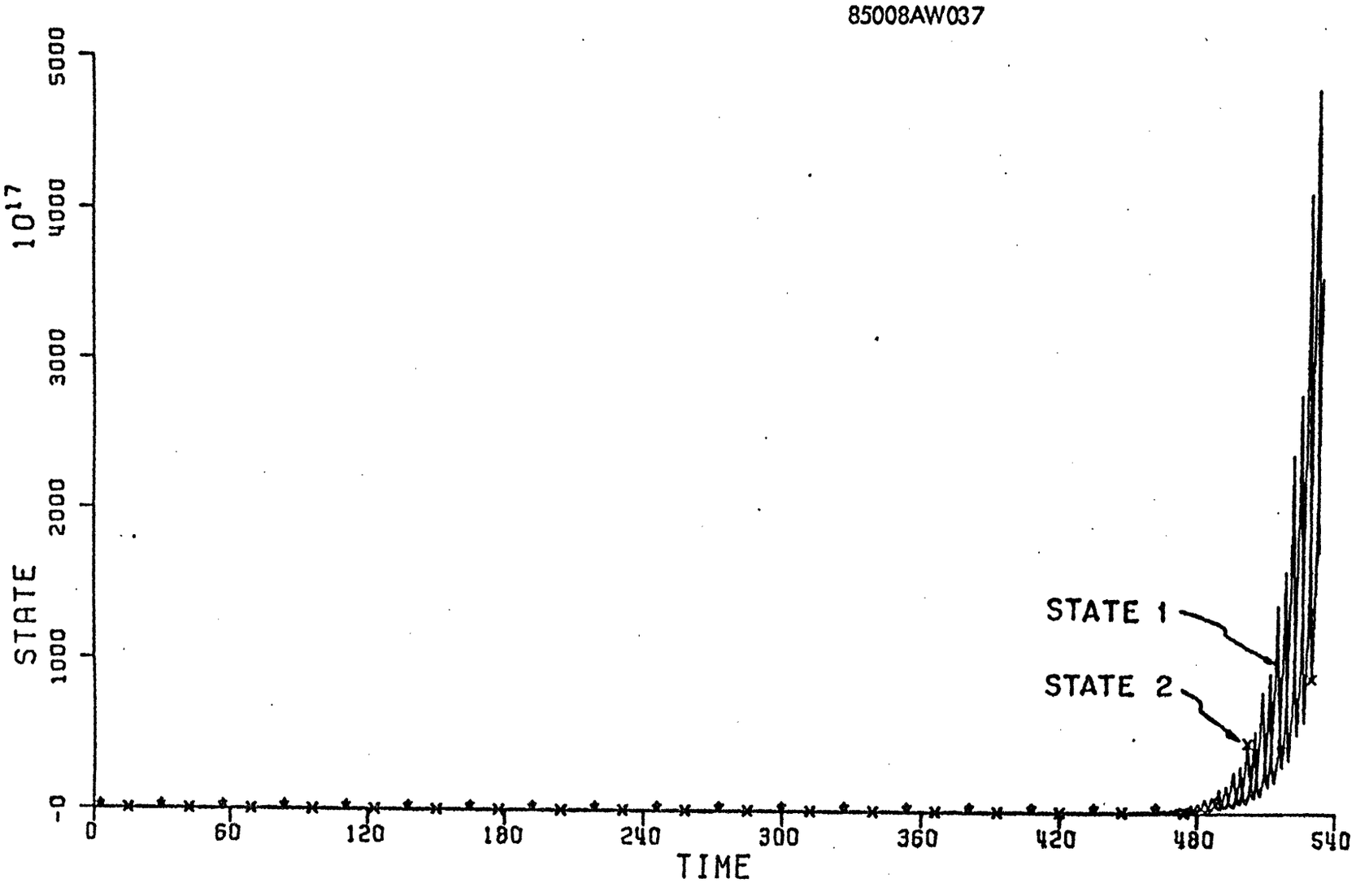


Fig. 3.4 Unstable Oscillation
(Case 1c)

b) True States

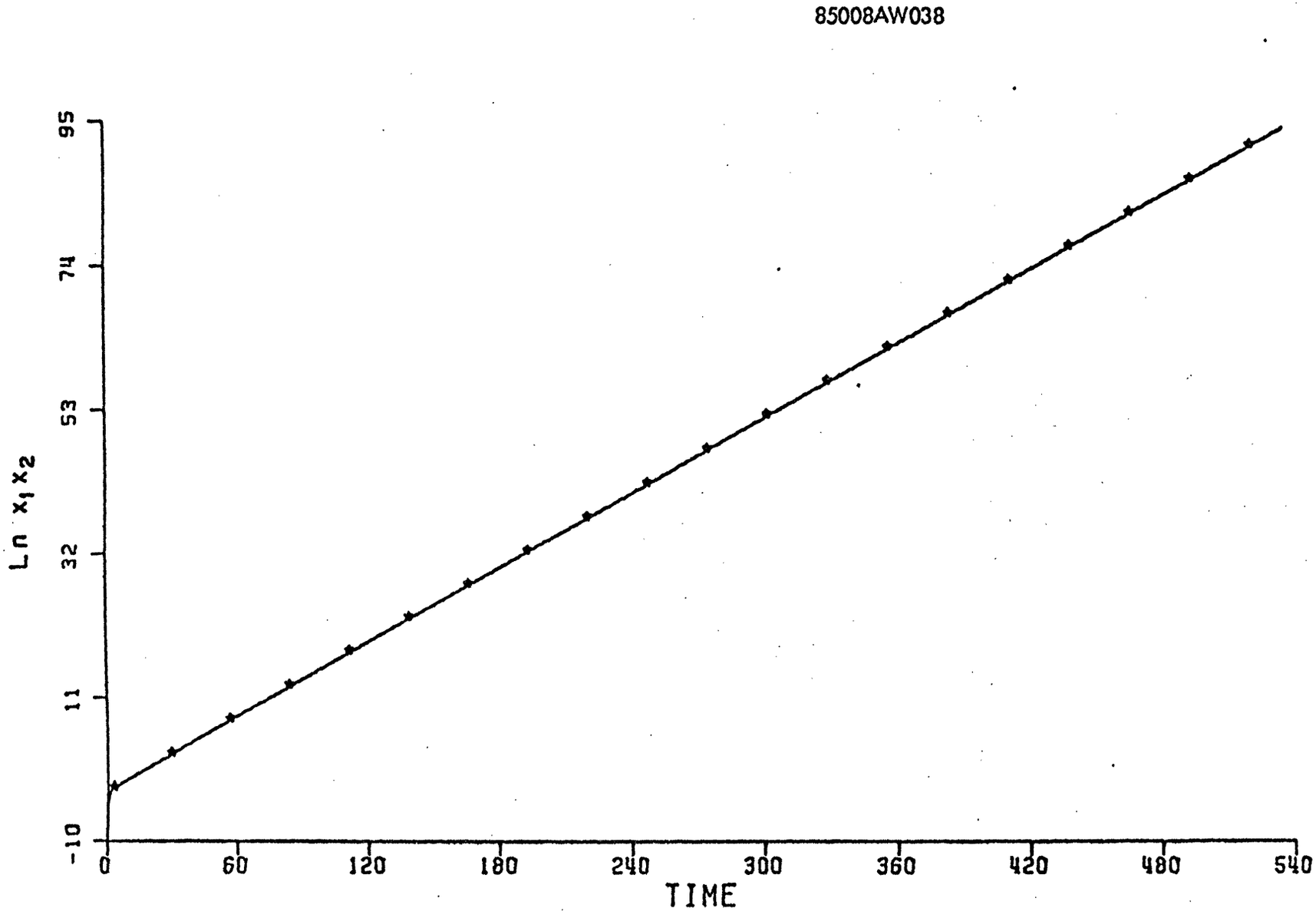


Fig. 3.4 Unstable Oscillation
(Case 1c)

c) Ln x_1x_2

exponentially. In [1] these cases are analyzed in detail, stability conditions are obtained, and approximate expressions for the switch times in p_1 are obtained. These equations predict the lengthing period observed in the stable example of Figure 3.2a.

Mixed Cases

If $\tilde{A}(p_1)$ is stable for some range of p_1 (which must be symmetric about $p_1=1/2$ by symmetry) but not for all p_1, one can obtain trajectories that display either type of behavior -- oscillatory or exponential -- depending upon the size of the initial condition. For large initial conditions, one can obtain some oscillation before the system settles. Also, there is a natural notion of domain of attraction . Let $(p_{min}, 1-p_{min})$ be the range of values of p_1 for which $\tilde{A}(p_1)$ is stable. Then for p_1 initially in this range, one can find a value $\varepsilon(p_1)$ so that if $||w|| < \varepsilon(p_1)$, p_1 always stays in this range. A technique for calculating an approximation to the domain of attraction is given in [1].

A number of other analytical techniques are described in [1]. In addition, a number of modifications to the MMAC algorithm are proposed and analyzed. One of the most promising of these is the limited memory MMAC, in which p_1 is calculated using only a window of the most recent filter residuals. What this does is speed up the response of p_1, and this leads to decreases in the peaks in x and an increase in the frequency of oscillation. This is illustrated in Figure 6.1. Note in this case that there is a limit cycle. In fact, limit cycles (with lower amplitude in x) are quite likely in this case. For example, note that if $w \to 0$ we must have $p_1 \to 1/2$ (since it is based on a finite window). However if $\tilde{A}(1/2)$ is unstable, this cannot happen. We refer the reader to [1] for details of the analysis of MMAC.

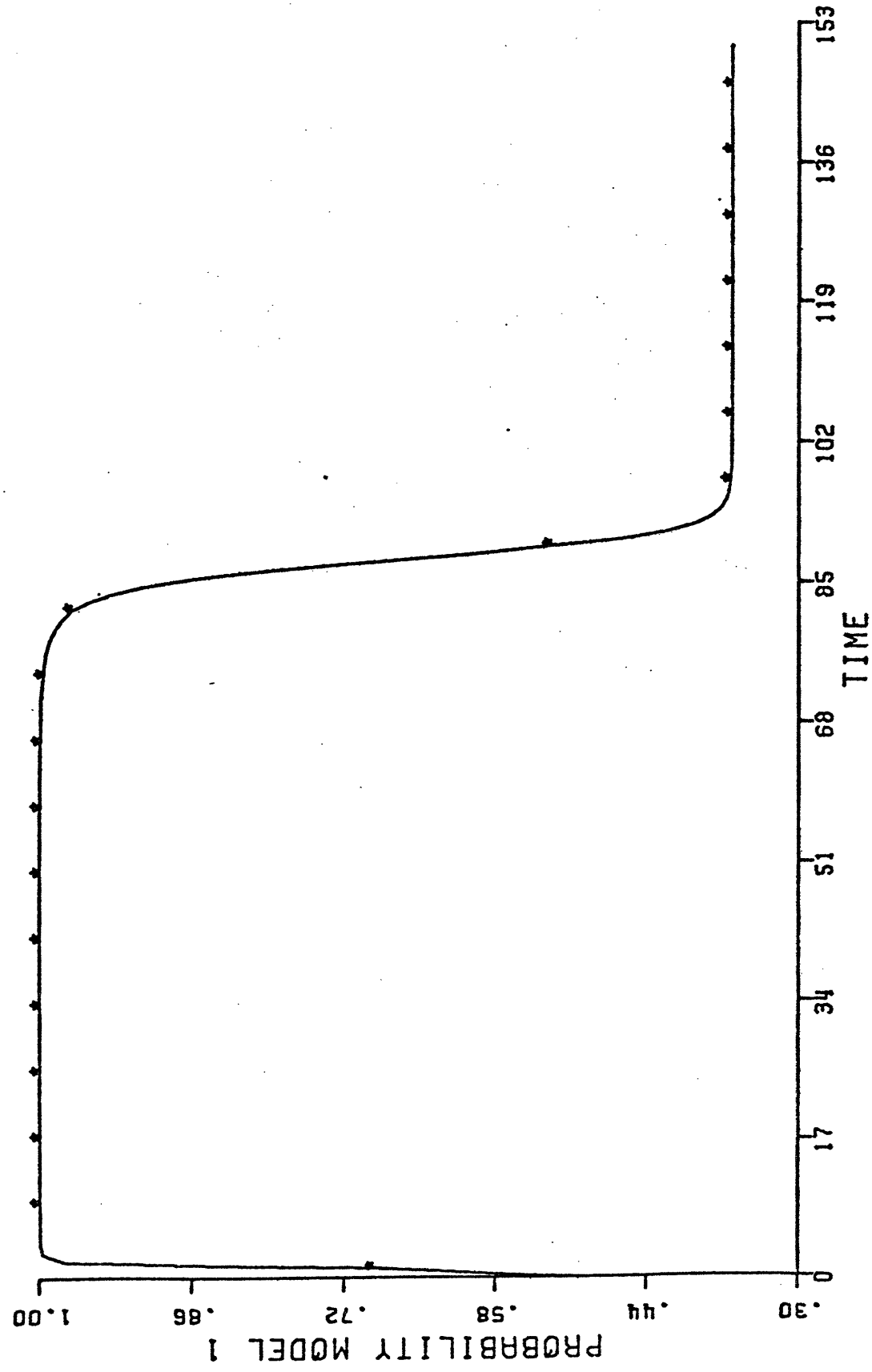


Fig. 3.6 Domain of Attraction - Large Initial Conditions (Case 2)

a) Probability of Model 1

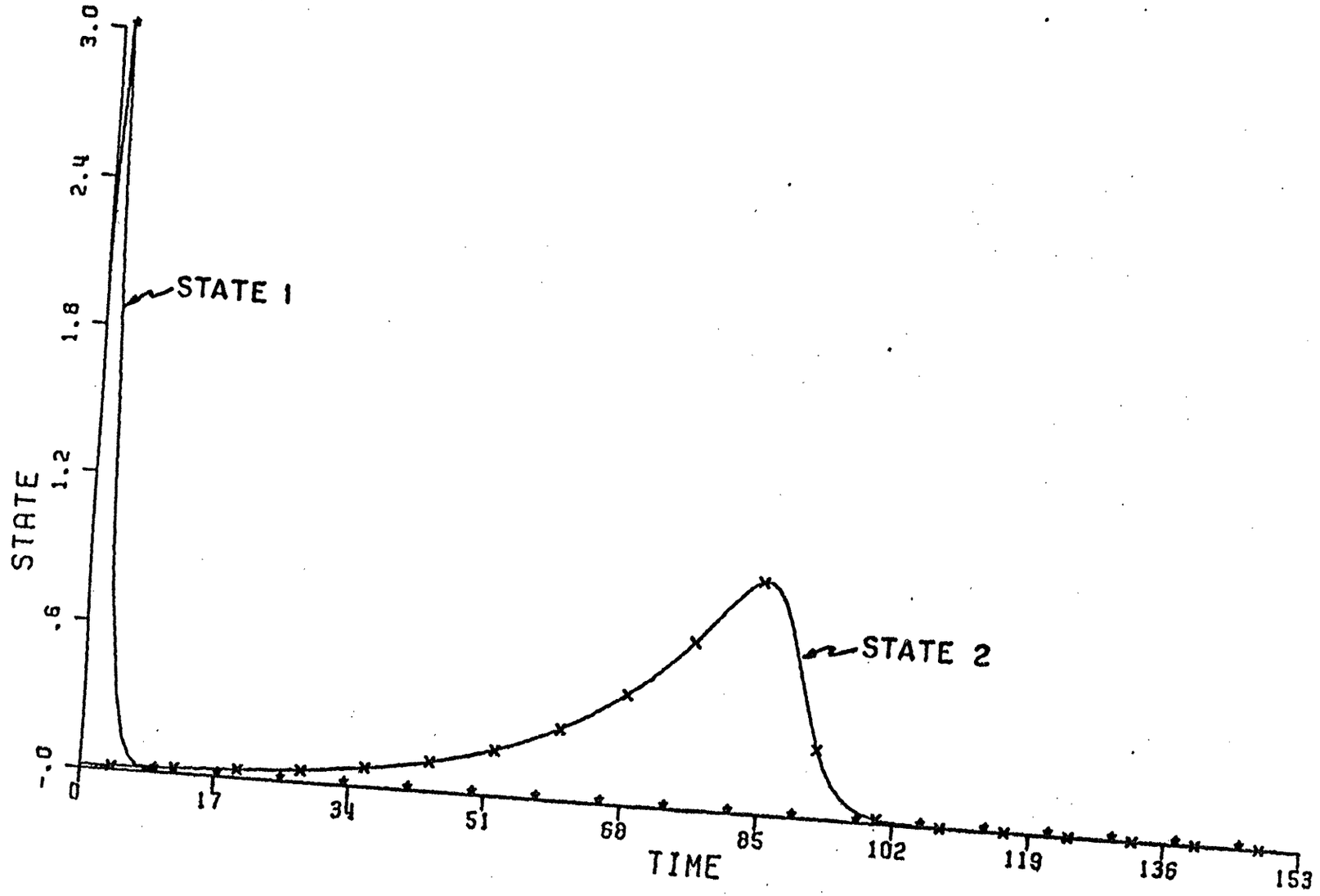


Fig. 3.6 Domain of Attraction - Large Initial Conditions (Case 2)

b) True States

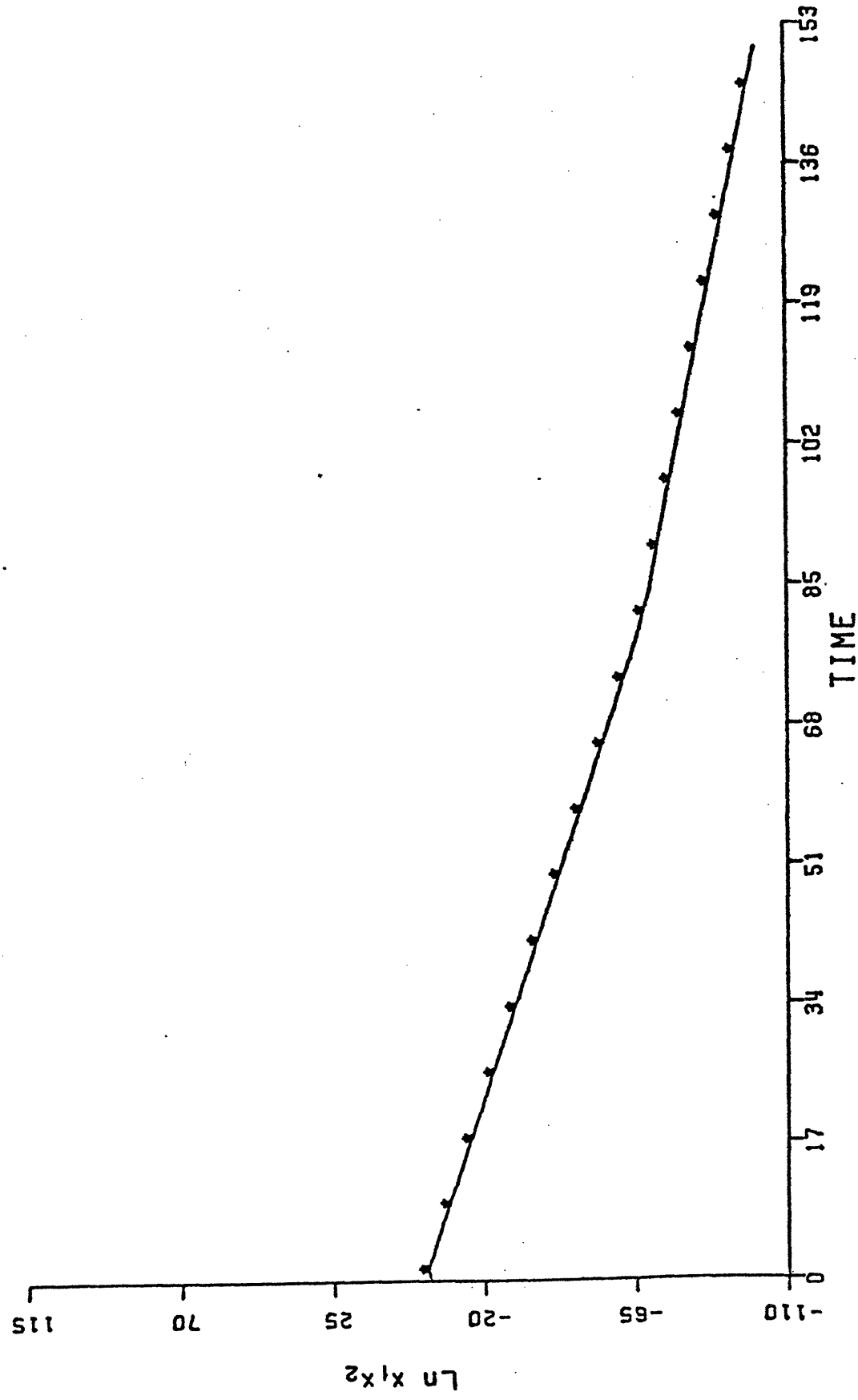


Fig. 3.6 Domain of Attraction - Large Initial Conditions (Case 2)

c) Ln x_1x_2

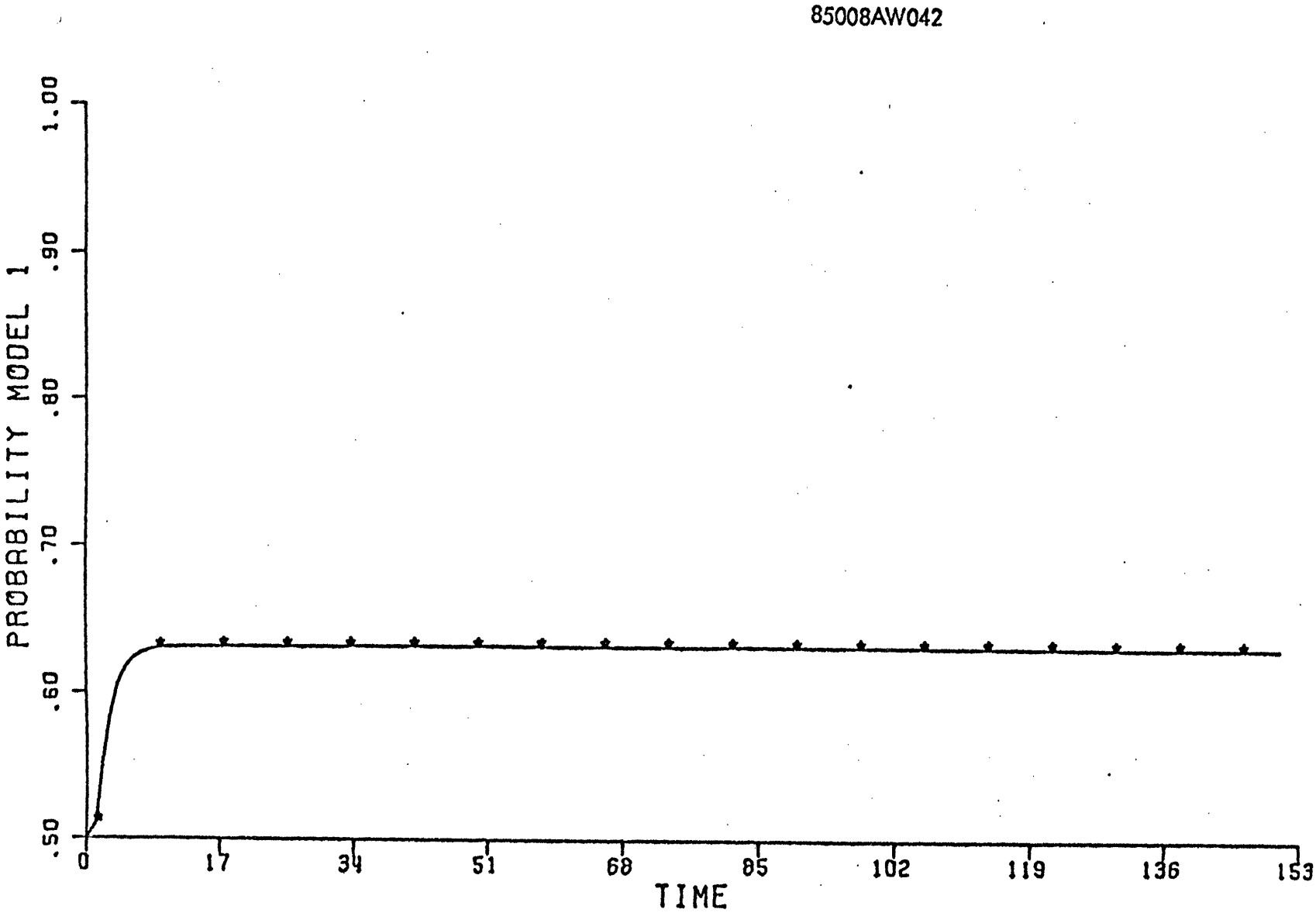


Fig. 3.7 Domain of Attraction - Small Initial Conditions (Case 2)

a) Probability of Model 1

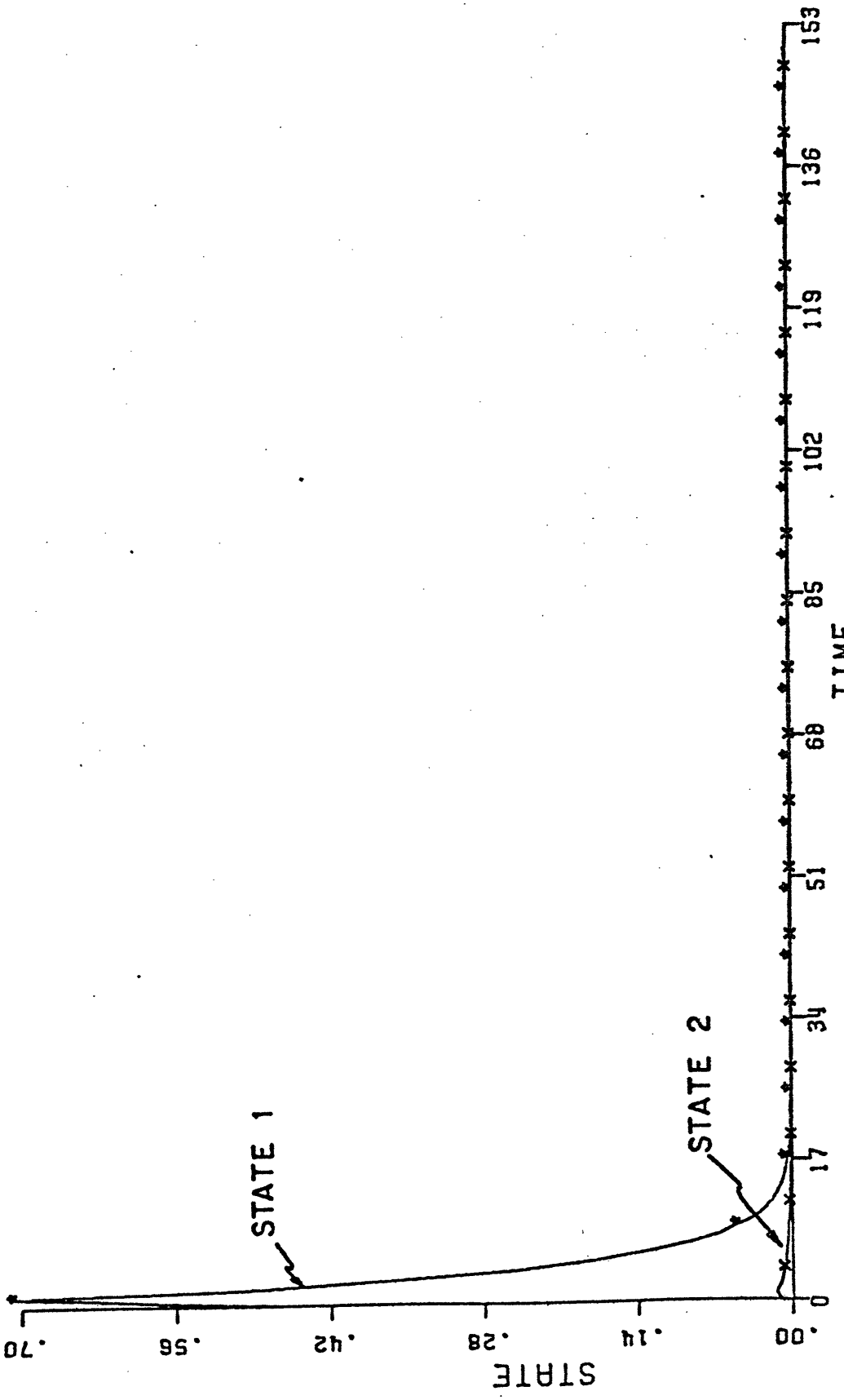


Fig. 3.7 Domain of Attraction - Small Initial Conditions (Case 2)

b) True States

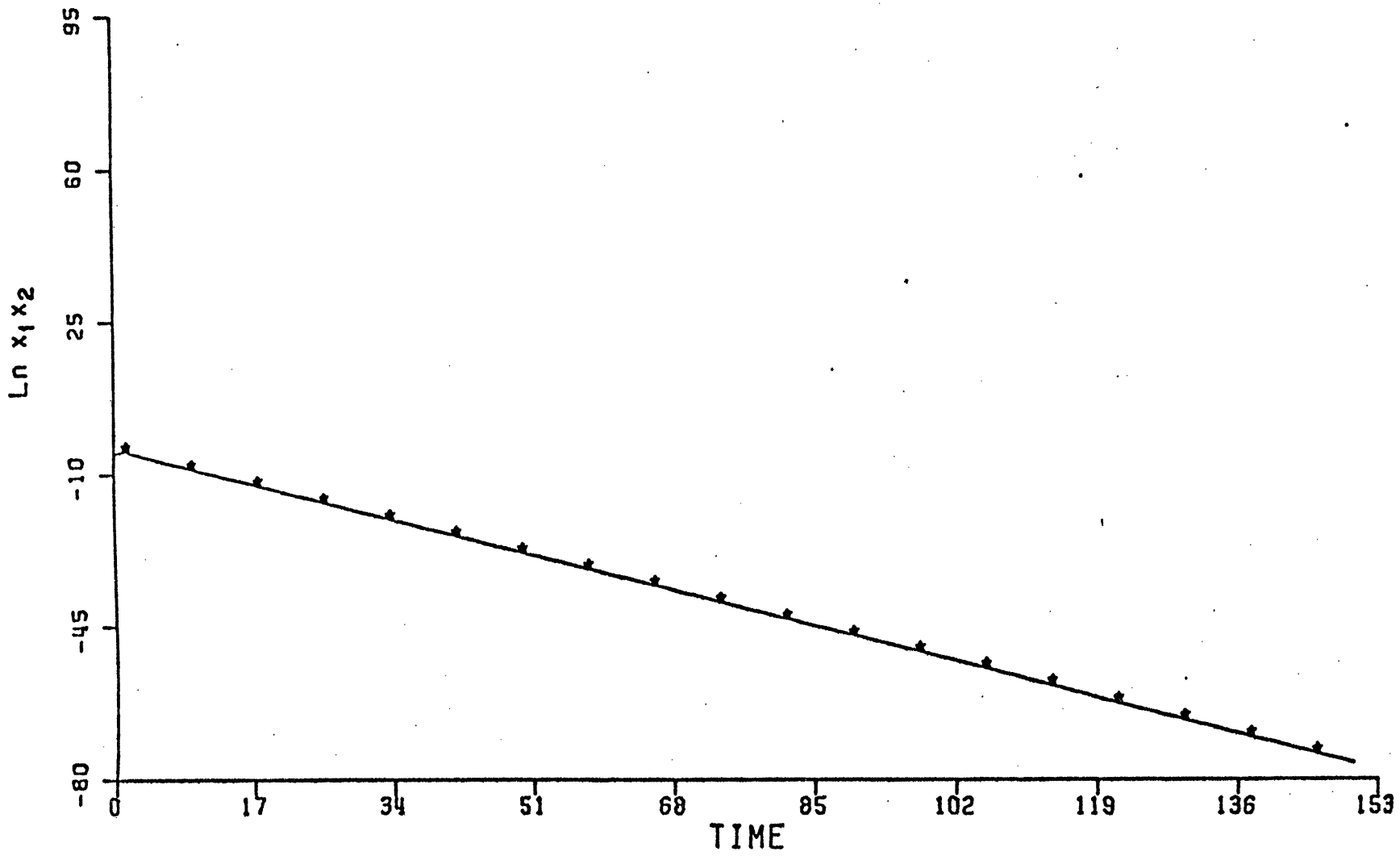


Fig. 3.7 Domain of Attraction - Small Initial Conditions (Case 2)

c) Ln $x_1 x_2$

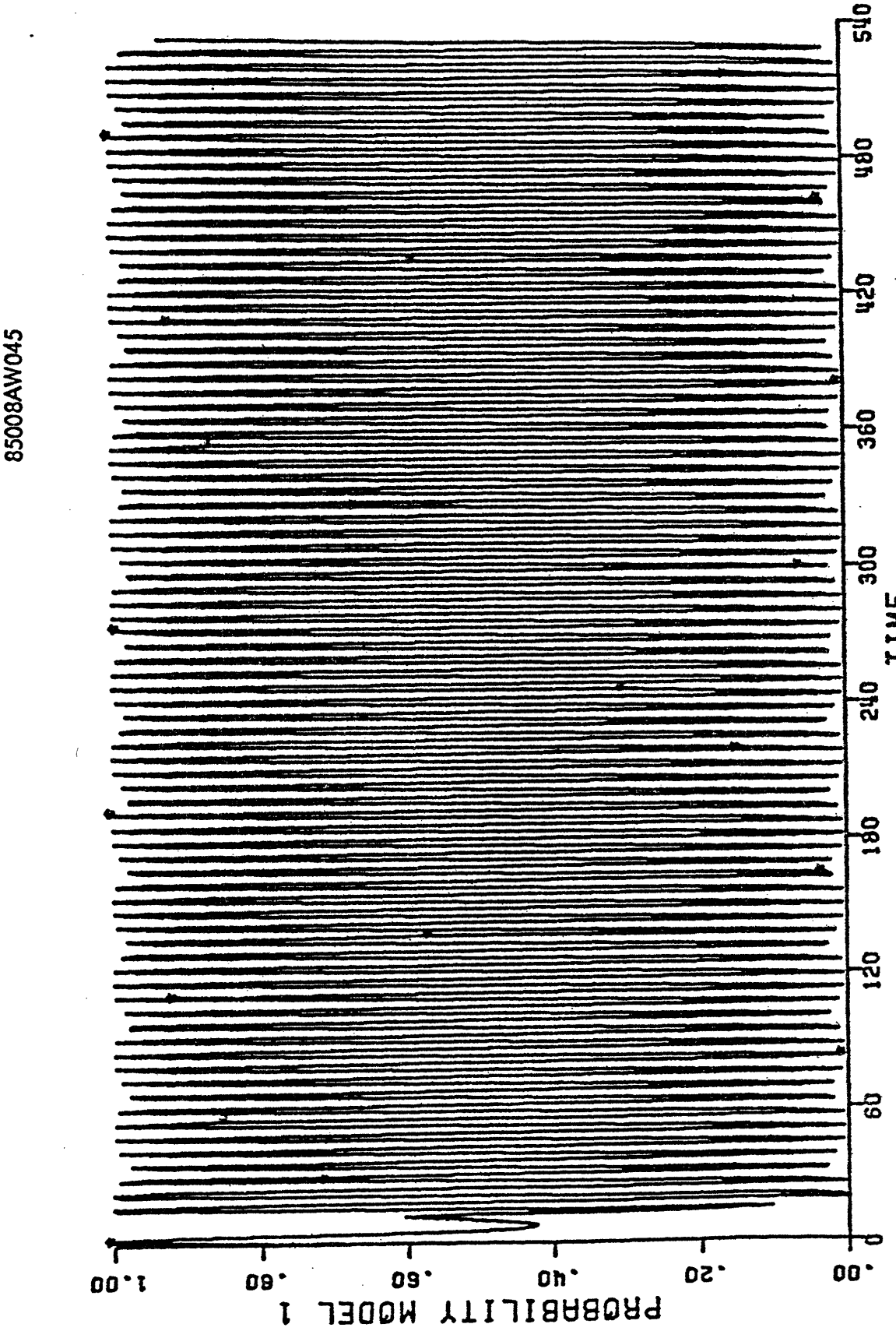


Fig. 6.1 Simulation of Finite Memory MMAC
(Case 1a with M=1)

a) Probability of Model 1

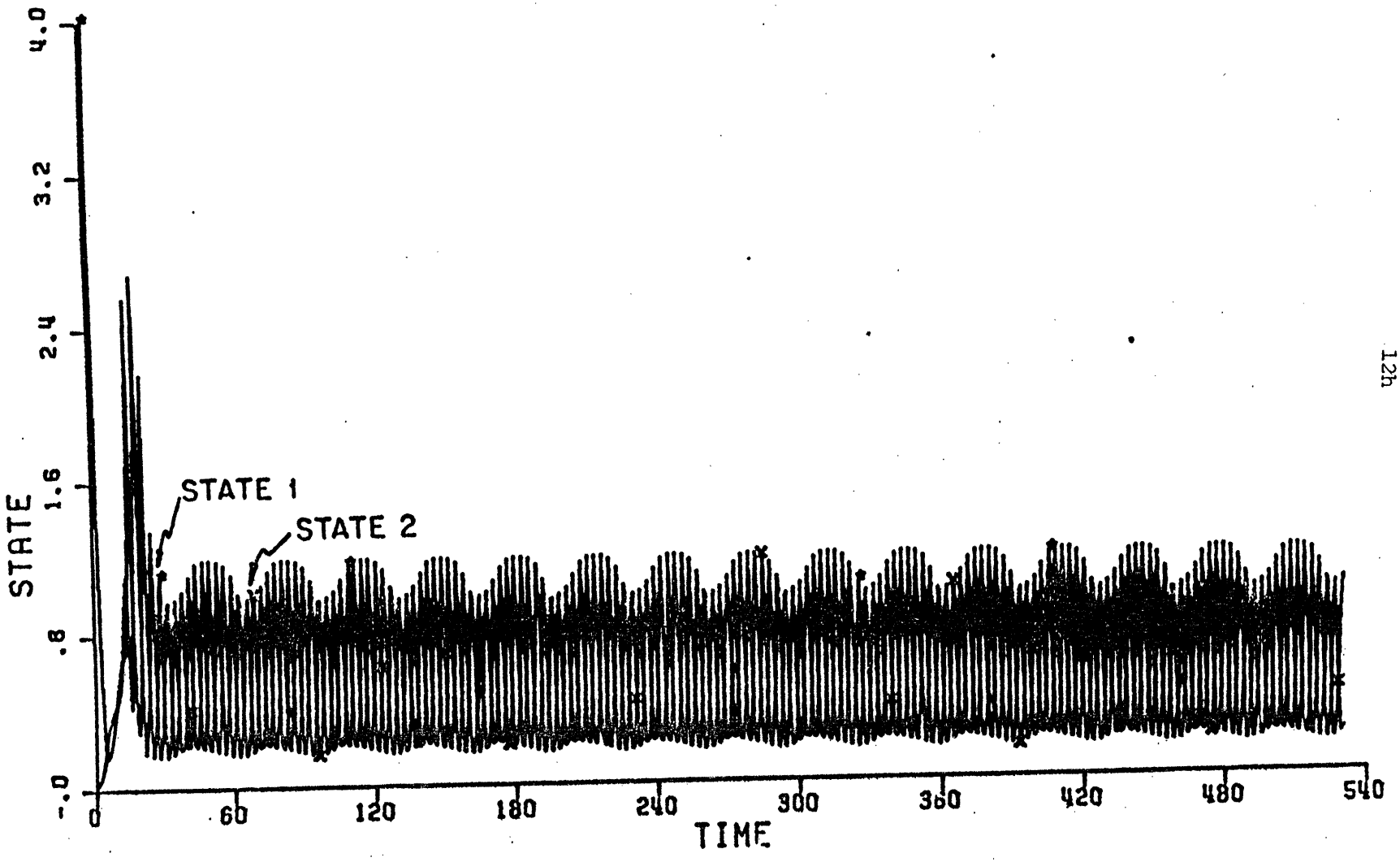


Fig. 6.1 Simulation of Finite Memory MMAC
(Case 1a with M=1)

b) True States

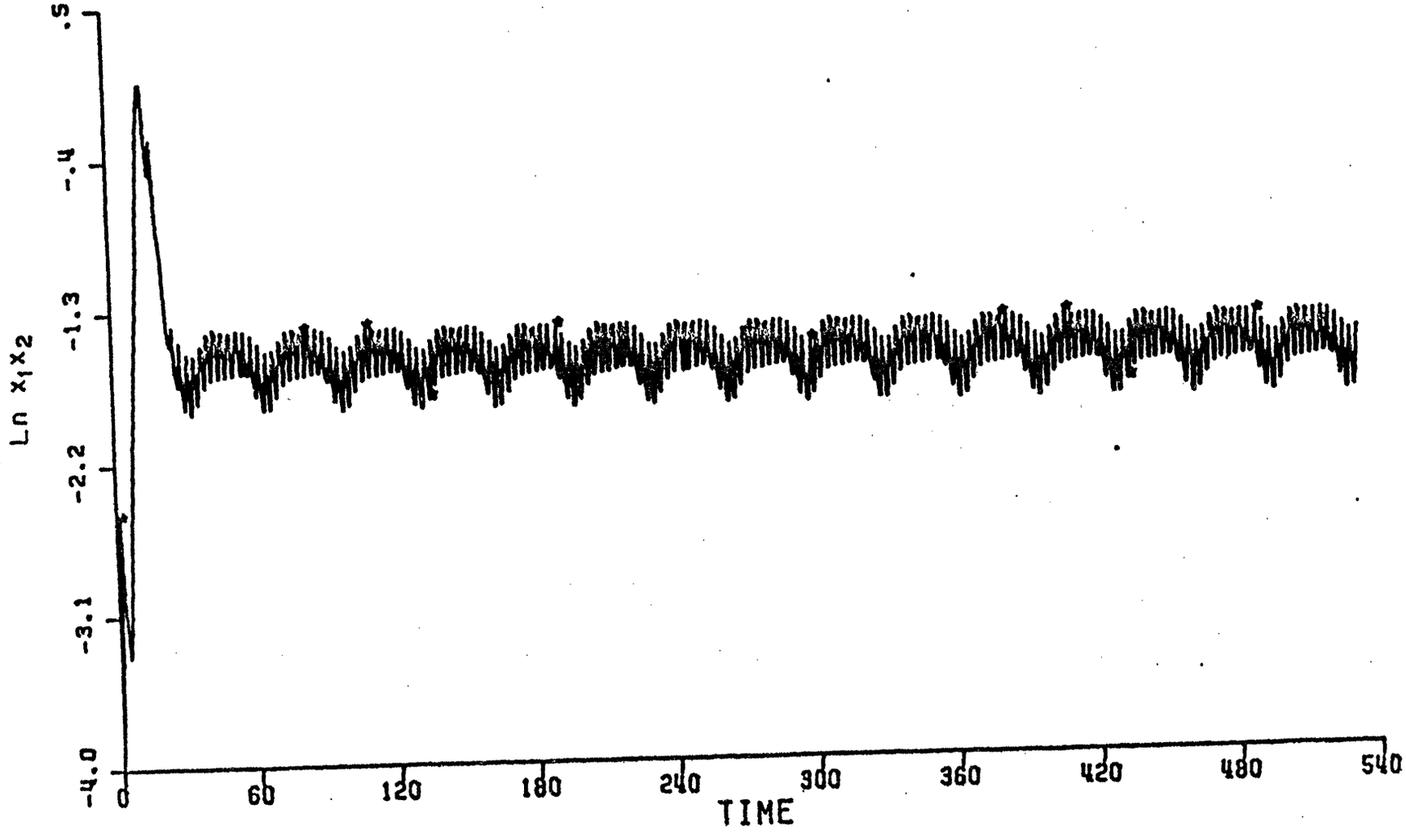


Fig. 6.1 Simulation of Finite Memory MMAC
(Case 1a with M=1)

c) Ln x_1x_2

II. The Design of Fault-Tolerant Control Systems

We have continued our work in developing a theory of fault-tolerant optimal control, in which the problems of adaptivity, hedging, and risk avoidance are built into the optimality criterion and problem formulation. The motivation here is to obtain a fundamental understanding of how to formulate fault-tolerant control system design problems. Specifically, we have begun to develop a framework for stochastic control problem formulation that leads to controllers that "optimize performance" prior to failure but "attempt to recover" or are "content to survive" subsequent to failure.

To date we have considered a sub-problem of the problem we eventually wish to consider. This work is summarized in [2]. Let $\rho(t)$ denote a finite-state jump process with state set $\{1,\ldots,N\}$. This process is used to denote the operational state of the system -- i.e. one of the values of ρ corresponds to normal operation, and the others denote degraded modes. Consider the system

$$\dot{x}(t) = A(\rho(t))x(t) + B(\rho(t))u(t) + C(\rho(t))w(t) \tag{43}$$

$$y(t) = C(\rho(t))x(t) + r(t) \tag{44}$$

where we assume that ρ is random but that its present value can be observed perfectly. We would like to design a controller to minimize the criterion

$$J = E\left\{\int_{t_o}^{t_1} [x'(s)Q(s,\rho(s))x(s) + u'(s)R(s,\rho(s))u(s)]ds + x'(T)K_T(\rho(T))x(T)\right\} \tag{45}$$

Here, by allowing Q,R, and K to depend on ρ, we can specify different objectives under different operating conditions. Sworder and his colleagues considered problems of this type when x is observed perfectly and when ρ is Markov. In this case the optimal control is of the form

$$u^*(t) = R^{-1}(t,j)B'(t,j)K(t,j)x(t) \quad \text{if } \rho(t)=j \tag{46}$$

where the K(t,j) satisfy Riccati-type equations that include "hedging" terms that reflect the fact that there may be different objectives in future operating modes.

In [2] these results are extended in several ways:

(1) If we observe y as in (44) instead of x, we obtain a separation/certainty - equivalence result.

(2) We can include jumps in x(t) at transition times for ρ and can also include "jump costs" at these times. These lead to modifications in the equations for K.

(3) We can consider the non-Markovian case for $\rho(t)$. The results become a bit more complicated but maintain their same basic form.

(4) We can allow some transitions in $\rho(t)$ to be controlled. The solution to this problem involves the comparison of several of the K(t,j). This problem is still being investigated.

The third of these extensions is particularly important, as operating condition transitions are not Markovian. The fourth extension allows the consideration of maintenance scheduling and decision rules for activating back-ups.

A great deal of work remains to be done in this area. Specifically, perfect observation of $\rho(t)$ is not realistic and one may also wish to consider transition probabilities for ρ that depend on x and u. If we assume that we have noisy observations of ρ or that we are to estimate its value from the observations y, we obtain a dual control problem. Although the optimal solution in this case may prove to be intractable, the work reported in [2] should provide us with some insights into the structure of useful designs. For example, we can view a failure detection system as providing an estimate $\hat{\rho}(t)$, which could be used in the control laws developed in [2]. This type of system and its relationship to the optimal will be examined in the future.

III. Development of a Failure Detection Methodology

Work in this area has proceeded along two lines. The first of these involves the development of "smart" detection rules using a Bayes' risk formulation. As described in [4], this formulation takes as its starting point the specification of failure signatures for each of the several failure hypotheses. The problem then is to obtain the optimal sequential decision rule, where the optimality criterion takes into account all of the important performance issues -- false alarm, detection delay, incorrect identification, etc.

In general the solution to this problem, the Bayes' sequential decision rule (BSDR) consists of two parts: 1) a stopping rule that tells us if we should stop taking observations and make a declaration of system status, and 2) a terminal decision rule that tells us what declaration to make. In general this rule can be quite complex. Thus, in order to gain some insight into its behavior, we have examined a special case in which the signature for each failure mode is constant and the observation noise is stationary. In this case the BSDR can be described as a function of the posterior distribution of each failure hypothesis given the observations. Consequently, we have sequential decision regions corresponding to each failure mode in the space of posterior distributions. The BSDR is simply: if at some point in time, the posterior distribution lies in one of these sequential decision regions, a declaration of the failure mode associated with that sequential decision region is made. If the distribution is not in any of these regions, decision is deferred. The decision regions are closed, convex sets, the exact shapes of which

depend on the cost and loss structure and the statistics of the observations. We have gained some insights into such dependence, based on which we are able to construct simpler but suboptimal sequential decision regions.

Based on our analysis of the BSDR for the simple case described above, we have begun to consider more complicated problems with time-varying signatures and unknown failure time. Several different tractable, suboptimal solutions have been proposed, and we plan to develop others that involve the concept of sequential decision regions in posterior distribution space. In conjunction with this, we will continue our development of methods for evaluating the performance of various decision rules. Several approaches to this problem are described in [4], and we plan to use these to evaluate the various decision rules that have been developed.

The second direction of our research has been aimed at the problem of sensor/actuator choice and the generation of signature-carrying signals to be used in BSDR's as described above. Conceptually, we can think of this aspect of our research as complementary to the part described previously. Basically, outputs of sensors can be used for the detection of failures in other sensors and actuators if there is a functional relationship between the instruments. Specifically, consider a system

$$\dot{x}(t) = Ax(t) + \sum_{i=1}^{M} b_i u_i(t) \tag{47}$$

$$y_i(t) = c_i' x(t) + v_i(t), \quad i=1,\ldots,P \tag{48}$$

where there are M possible actuators and P possible sensors (some of which must be identical). Consider the subspaces

$$S_i = \text{Range}[b_i \mid Ab_i \mid \ldots \mid A^{n-1}b_i] \tag{49}$$

$$T_i = \text{Range}[c_i \mid A'c_i \mid \ldots \mid (A')^{n-1}c_i] \tag{50}$$

A number of concepts related to reliability and failure detection can be deduced from these matrices. For example, the system can tolerate an ith actuator failure (assuming that all M actuators are used) if

$$R^n = \bigoplus_{j \neq i} S_j \tag{51}$$

Also, the ith sensor can be used to help in the detection of the jth actuator if

$$S_j \cap T_i \neq \{0\} \tag{52}$$

and it can be compared usefully to the jth sensor if

$$T_j \cap T_i \neq \{0\} \tag{53}$$

Since one needs another piece of information to distinguish failures of sensor i and j, we come naturally to the fact that a failure in sensor i is detectable if there are two other sensors, j and k such that

$$T_i \cap T_j \neq \{0\} \quad \text{and} \quad T_i \cap T_k \neq \{0\} \tag{54}$$

The use of geometric concepts such as these to aid in the design of failure detection systems goes back to the work of Beard [5] and Jones [6]. We have begun to build on their work to study two problems:

(1) The sensor selection problem. Which sensors do we use to achieve a certain level of performance. Since performance must include the effect of the failure detection system, this work must be tied in with our analysis of BSDR's for failure detection.

(2) The generation of signature - carrying residual processes. The GLR system described in [4] produces residuals by implementing a Kalman filter for the entire state. The signatures then can be calculated as the response of the plant-filter combination to the failure. This approach runs into difficulties if some system parameters are not known well. We plan to use a geometric approach to overcome this problem.

The basic idea behind (2) has recently been developed. Consider the system (47), (48), and suppose, for simplicity, that we are only interested in sensor failures. Suppose that the c_i are known, but that A depends upon some unknown parameters. Consider failure detection for sensor i, and consider a sensor j that satisfies (53). The question is: is this comparison a useful comparison? Clearly it is if A restricted to $T_i \cap T_j$ is known perfectly. It is this observation that we plan to use in order

to build robust failure detection systems. Specifically, we plan to develop procedures for decomposing systems into lower dimensional subsystems, involving only a subset of the sensors. One can then apply the usual Kalman filter - GLR techniques in order to generate parameter-insensitive, signature-carrying residuals.

IV. Detection of Sequences of Events

Recently we initiated a study of a related topic, involving the detection of a series of events, in which there is some probabilistic description for the sequence of events, such as that discussed in Section II. Consider a finite-state process $\rho(t) \in \{1,\ldots,N\}$, and with each state, associated a characteristic signal or waveform $S_i(t)$, $i=1,\ldots,N$. Let $\tau(t)$ denote the elapsed time since the last transition of $\rho(t)$. Then our observation is

$$y(t) = S_{\rho(t)}(\tau(t)) + v(t) \tag{55}$$

Intuitively, when we enter the state $\rho(t)=i$, we begin to transmit the characteristic signature S_i.

At this time, we have analyzed the problem of estimating ρ and τ given y assuming that for $i \neq j$

$$\text{Prob}[\rho(t+\Delta)=i \,|\, \rho(t)=j,\ \tau(t)=\tau] = \lambda_{ji}(\tau)\Delta + o(\Delta) \tag{56}$$

(note that ρ is <u>not</u> Markov here, as λ_{ji} depends on τ), and that the S_i are deterministic. In general this is a nonlinear filtering problem, and we have derived the equations for the evolution of the conditional distribution. Future work will include deriving efficient suboptimal estimators and in considering stochastic models for the $S_i(t)$ and more general models for $\rho(t)$, such as as a semi-Markov process (the sequence of <u>values</u> of $\rho(t)$ is Markov, but the transition times need not be).

PERSONNEL

During this time period Prof. Alan S. Willsky (principal investigator), Dr. Stanley B. Gershwin, and Prof. Gunter Stein[1] have been involved in the research outlined in this status report. In addition, four students have worked on these problems. Mr. C.S. Greene's Ph.D. thesis [1] consisted of the work described in Section I. Mr. H. Chizeck has been working on the problems discussed in Section II, Mr. E.Y. Chow has been responsible for the research in Section III, and Mr. J.-Y. Wang is working in the area described in Section IV. Greene and Chow have been research assistants under this project..

---

[1] Prof. Stein received no financial support under this contract.

References

(Reference numbers with asterisks report work performed in part under this contract).

*1. C.S. Greene, "An Analysis of the Multiple Model Adaptive Control Algorithm," Report ESL-TH-843, Ph.D. thesis, M.I.T., August 1978.

*2. H. Chizeck and A.S. Willsky, "Towards Fault-Tolerant Optimal Control," Proc. IEEE Conf. on Decision and Control, San Diego, Calif., Jan. 1979.

*3. C.S. Greene and A.S. Willsky, "Deterministic Stability Analysis of the Multiple Model Adaptive Control Algorithm," in preparation.

4. "Status Report Number One, on the Development of a Methodology for the Detection of System Failures and for the Design of Fault-Tolerant Control Systems," Rept. ESL-SR-781, Nov. 15, 1977.

5. R.V. Beard, "Failure Accomodation in Linear Systems Through Self-Reorganization," Rept. MVL-71-1, Man-Vehicle Lab., M.I.T., Cambridge, Mass., Feb. 1971.

6. H.L. Jones, "Failure Detection in Linear Systems," Ph.D. thesis, Dept. of Aeronautics and Astronautics, M.I.T., Camb., Mass., Sept. 1973.